

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION of
Inventor(s): Saori NISHIMURA

Appln. No.: _____
Series Code ↑ ↑ Serial No.

Group Art Unit: Not Yet Assigned

1c821 U.S. PTO
09/976050
10/15/01

Filed: Herewith

Examiner: Not Yet Assigned

Title: IC CARD TERMINAL UNIT AND IC CARD DUPLICATION METHOD

Atty. Dkt. P 282732 T4IA-01S0063-1
M# Client Ref

Date: October 15, 2001

**SUBMISSION OF PRIORITY
DOCUMENT IN ACCORDANCE
WITH THE REQUIREMENTS OF RULE 55**

Hon. Asst Commissioner of Patents
Washington, D.C. 20231

Sir:

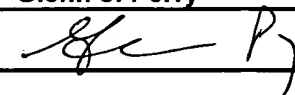
Please accept the enclosed certified copy(ies) of the respective foreign application(s) listed below for which benefit under 35 U.S.C. 119/365 has been previously claimed in the subject application and if not is hereby claimed.

<u>Application No.</u>	<u>Country of Origin</u>	<u>Filed</u>
2001-043630	JAPAN	February 20, 2001

Respectfully submitted,

Pillsbury Winthrop LLP
Intellectual Property Group

1600 Tysons Boulevard
McLean, VA 22102
Tel: (703) 905-2000

By Atty: Glenn J. Perry Reg. No. 28458
Sig:  Fax: (703) 905-2500
Tel: (703) 905-2161

Atty/Sec: gjp/vaw

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

#2
Jc821 U.S. PRO
09/976050
10/15/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

2001年 2月20日

出願番号

Application Number:

特願2001-043630

出願人

Applicant (s):

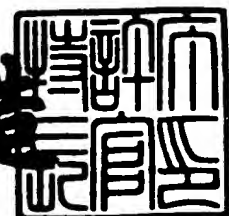
株式会社東芝

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 3月16日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2001-3020962

【書類名】 特許願

【整理番号】 A000007563

【提出日】 平成13年 2月20日

【あて先】 特許庁長官 殿

【国際特許分類】 G06K 17/00

【発明の名称】 I C カード、I C カード端末装置および I C カード複製
方法

【請求項の数】 13

【発明者】

 【住所又は居所】 神奈川県川崎市幸区柳町 7 0 番地 株式会社東芝柳町事
業所内

 【氏名】 西村 佐織

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

 【氏名又は名称】 村松 貞男

【選任した代理人】

 【識別番号】 100068814

 【弁理士】

 【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ICカード、ICカード端末装置およびICカード複製方法

【特許請求の範囲】

【請求項1】 外部装置との間でデータを通信する通信手段と、
少なくともデータを暗号化あるいは復号化するための第1の鍵を記憶している記憶手段と、

前記通信手段を介して受信されたデータが鍵設定命令である場合、この鍵設定命令に付加された第2の鍵を前記記憶手段に記憶せしめる鍵設定手段と、

前記通信手段を介して受信されたデータが鍵取出命令である場合、前記鍵設定手段により前記記憶手段に記憶された第2の鍵で前記記憶手段内の第1の鍵を暗号化し、この暗号化した第1の鍵を前記通信手段を介して外部へ出力する鍵出力手段と、

を具備したことを特徴とするICカード。

【請求項2】 前記記憶手段内の第1の鍵は、前記通信手段を介して外部から入力された鍵生成命令に基づき該ICカード内で生成されたものであることを特徴とする請求項1記載のICカード。

【請求項3】 前記記憶手段内の第1の鍵は、外部で生成され、前記通信手段を介して外部から入力されたものであることを特徴とする請求項1記載のICカード。

【請求項4】 前記鍵設定命令は、該ICカードの発行者によって前記通信手段を介して外部から入力されたものであることを特徴とする請求項1記載のICカード。

【請求項5】 前記鍵設定命令は、該ICカードの所持者によって前記通信手段を介して外部から入力されたものであることを特徴とする請求項1記載のICカード。

【請求項6】 一方には少なくともデータを暗号化あるいは復号化するための鍵が記憶され、他方には該鍵が記憶されていない2つのICカードとの間でデータを通信する通信手段と、

前記鍵が記憶された一方のＩＣカードに対し鍵取出命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内の鍵を前記通信手段を介して取出す鍵取出手段と、

前記鍵が記憶されていない他方のＩＣカードに対し前記鍵取出手段により前記一方のＩＣカードから取出した鍵を付加した暗号鍵設定命令を前記通信手段を介して送信することにより、該鍵を前記他方のＩＣカード内に記憶せしめる暗号鍵設定手段と、

を具備したことを特徴とするＩＣカード端末装置。

【請求項 7】 2つのＩＣカードとの間でデータを通信する通信手段と、

前記 2つのＩＣカードに対し、第 1の鍵を暗号化あるいは復号化するための第 2の鍵を付加した鍵設定命令を前記通信手段を介して送信することにより、該第 2の鍵を前記 2つのＩＣカード内にそれぞれ記憶せしめる第 1の鍵設定手段と、

この第 1の鍵設定手段による前記第 2の鍵の設定が正常に終了したことを確認する確認手段と、

この確認手段により第 2の鍵の設定が正常に終了したことが確認されると、前記 2つのＩＣカードのうち一方のＩＣカードに対し鍵生成命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内においてデータを暗号化あるいは復号化するための前記第 1の鍵を生成せしめる鍵生成手段と、

この鍵生成手段により第 1の鍵を生成させた前記一方のＩＣカードに対し鍵取出命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内で生成された第 1の鍵を前記通信手段を介して取出す鍵取出手段と、

前記 2つのＩＣカードのうち他方のＩＣカードに対し前記鍵取出手段により前記一方のＩＣカードから取出した第 1の鍵を付加した暗号鍵設定命令を前記通信手段を介して送信することにより、該第 1の鍵を前記他方のＩＣカード内に記憶せしめる第 2の鍵設定手段と、

を具備したことを特徴とするＩＣカード端末装置。

【請求項 8】 少なくともデータを暗号化あるいは復号化するための鍵が記憶されている被複製用の第 1のＩＣカードと、複製用の第 2のＩＣカードと、これら第 1、第 2のＩＣカードを取扱う端末装置とを有し、

前記端末装置から前記第 1 の I C カードに対し鍵取出命令を送信する第 1 のステップと、

前記第 1 の I C カードにおいて、前記端末装置から送信された鍵取出命令を受信し、前記鍵を前記端末装置に対し送信する第 2 のステップと、

前記端末装置において、前記第 1 の I C カードから送信された鍵を受信し、この受信した鍵を付加した暗号鍵設定命令を前記第 2 の I C カードに対し送信する第 3 のステップと、

前記第 2 の I C カードにおいて、前記端末装置から送信された暗号鍵設定命令を受信し、その暗号鍵設定命令に付加された鍵を記憶する第 4 のステップと、

を具備したことを特徴とする I C カード複製方法。

【請求項 9】 前記第 1 の I C カードに記憶されているデータを暗号化あるいは復号化するための鍵は、前記端末装置から入力された鍵生成命令に基づき該第 1 の I C カード内で生成されたものであることを特徴とする請求項 8 記載の I C カード複製方法。

【請求項 10】 前記第 1 の I C カードに記憶されているデータを暗号化あるいは復号化するための鍵は、外部で生成され、前記端末装置を介して入力されたものであることを特徴とする請求項 8 記載の I C カード複製方法。

【請求項 11】 少なくともデータを暗号化あるいは復号化するための第 1 の鍵が記憶されている被複製用の第 1 の I C カードと、複製用の第 2 の I C カードと、これら第 1、第 2 の I C カードを取扱う端末装置とを有し、

前記端末装置から前記第 1、第 2 の I C カードに対し、前記第 1 の鍵を暗号化あるいは復号化するための第 2 の鍵を付加した鍵設定命令を送信する第 1 のステップと、

前記第 1、第 2 の I C カードにおいて、前記端末装置から送信された鍵設定命令を受信し、その鍵設定命令に付加された第 2 の鍵をそれぞれ記憶する第 2 のステップと、

前記端末装置から前記第 1 の I C カードに対し鍵取出命令を送信する第 3 のステップと、

前記第 1 の I C カードにおいて、前記端末装置から送信された鍵取出命令を受

信し、前記第 2 のステップで記憶された第 2 の鍵により前記第 1 の鍵を暗号化し、この暗号化した第 1 の鍵を前記端末装置に対し送信する第 4 のステップと、

前記端末装置において、前記第 1 の IC カードから送信された暗号化された第 1 の鍵を受信し、この受信した暗号化された第 1 の鍵を付加した暗号鍵設定命令を前記第 2 の IC カードに対し送信する第 5 のステップと、

前記第 2 の IC カードにおいて、前記端末装置から送信された暗号鍵設定命令を受信し、その暗号鍵設定命令に付加された暗号化された第 1 の鍵を前記第 2 のステップで記憶された第 2 の鍵により復号化し、この復号化した第 1 の鍵を記憶する第 6 のステップと、

を具備したことを特徴とする IC カード複製方法。

【請求項 1 2】 前記第 1 の IC カードに記憶されているデータを暗号化あるいは復号化するための第 1 の鍵は、前記端末装置から入力された鍵生成命令に基づき該第 1 の IC カード内で生成されたものであることを特徴とする請求項 1 記載の IC カード複製方法。

【請求項 1 3】 前記第 1 の IC カードに記憶されているデータを暗号化あるいは復号化するための第 1 の鍵は、外部で生成され、前記端末装置を介して入力されたものであることを特徴とする請求項 1 記載の IC カード複製方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、たとえば、内部で生成したデータを暗号化あるいは復号化するための鍵を別の鍵で暗号化して外部へ取出すことのできる IC カードに関する。

【0002】

また、本発明は、上記 IC カードを用いてその複製カード（たとえば、バックアップカード）を作成する IC カード端末装置および IC カード複製方法に関する。

【0003】

【従来の技術】

最近、携帯可能な記憶媒体として、不揮発性のデータメモリとそれを制御する

ためのCPU（セントラル・プロセッシング・ユニット）を有するICチップを内蔵した、いわゆるICカードが産業各方面で利用されてきている。

【0004】

この種のICカードは、通常、カード発行会社などに設置されているICカード発行装置を用いて発行される。このICカード発行装置では、ICカードを機能させるのに必要な命令データ、磁気エンコードデータ、印刷データなどをホストコンピュータにより作成し、それを発行機に順次伝送し、命令データについては、ICカード内のICチップへ入力し、磁気エンコードデータおよび印刷データについては、ICカードの表面に磁気記録および印刷するようにしている。

【0005】

ICカード内のICチップに対する命令データに伴い実行される処理は、ICカード発行処理の上で最も重要な処理の1つである。ICカード内のICチップは、伝送された個々の命令データの処理が正常に行なえたか否かの情報を出力する手段を備えていて、発行装置はICチップからの出力情報を基に命令データを正常に伝送できたか否かを判断する手段を備えている。

【0006】

また、ICカードは、高いセキュリティを確保するために複数の鍵をデータメモリに設定記憶し、この複数の鍵を利用してデータの隠蔽やデータの正当性の確認処理などを行なうようになっている。

【0007】

さらに、最近、たとえば、ネットワークにつながれた複数のパーソナルコンピュータのセキュリティを高めるために、ICカードを利用する方法が開発されており、ICカード内に記憶された鍵を利用して、電子データファイルの隠蔽やデータの正当性の確認処理などを行なう方法が利用されている。

【0008】

また、より高いセキュリティを確保するために、複数の鍵をICカード内のCPUで生成することにより、鍵設定時の外部への漏洩を防止する方法がとられている。

【0009】

【発明が解決しようとする課題】

ところが、上述した複数の鍵をＩＣカード内で生成する従来のＩＣカードシステムにおいて、ＩＣカードが破壊されたり、ＩＣカードを紛失したりすると、ＩＣカード内で生成した複数の鍵を利用して隠蔽や正当性の確認などを行なった電子データファイルを使用できなくなるという問題があった。

【0010】

また、ＩＣカード内で生成した複数の鍵を容易にＩＣカード外に取出すことができると、セキュリティが著しく低下するという問題があった。

【0011】

そこで、最近、たとえば、特開 2 0 0 0 - 2 6 8 1 3 7 号公報に開示されているようなＩＣカードのバックアップ方法が考えられている。このＩＣカードのバックアップ方法は、正規のＩＣカードを識別するための識別情報を含むカード情報を、正規のＩＣカードから予備のＩＣカード内に複写しておき、必要に応じて、この予備のＩＣカードを正規のＩＣカードとする内容に上記識別情報を変更して、予備のＩＣカードを正規のＩＣカードに変更することにより、ＩＣカードの再発行を行なう技術である。

【0012】

しかし、このＩＣカードのバックアップ方法は、全く同じＩＣカードを複製するものではない。したがって、再発行されたＩＣカードを用いても、前述したような問題を解決することはできない。

【0013】

本発明は、上記課題を解決するためになされたもので、内部に記憶された、データを暗号化あるいは復号化するための鍵を安全に外部へ取出すことのできるＩＣカードを提供することを目的とする。

【0014】

また、本発明は、ＩＣカード内に記憶された、データを暗号化あるいは復号化するための鍵を安全に外部へ取出し、それを別のＩＣカード内に記憶することにより、その複製カード（たとえば、バックアップカード）を容易に作成することのできるＩＣカード端末装置およびＩＣカード複製方法を提供することを目的と

する。

【 0 0 1 5 】

【課題を解決するための手段】

本発明のＩＣカードは、外部装置との間でデータを通信する通信手段と、データを暗号化あるいは復号化するための第１の鍵を記憶している記憶手段と、前記通信手段を介して受信されたデータが鍵設定命令である場合、この鍵設定命令に付加された第２の鍵を前記記憶手段に記憶せしめる鍵設定手段と、前記通信手段を介して受信されたデータが鍵取出命令である場合、前記鍵設定手段により前記記憶手段に記憶された第２の鍵で前記記憶手段内の第１の鍵を暗号化し、この暗号化した第１の鍵を前記通信手段を介して外部へ出力する鍵出力手段とを具備している。

【 0 0 1 6 】

また、本発明のＩＣカード端末装置は、一方には少なくともデータを暗号化あるいは復号化するための鍵が記憶され、他方には該鍵が記憶されていない２つのＩＣカードとの間でデータを通信する通信手段と、前記鍵が記憶された一方のＩＣカードに対し鍵取出命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内の鍵を前記通信手段を介して取出す鍵取出手段と、前記鍵が記憶されていない他方のＩＣカードに対し前記鍵取出手段により前記一方のＩＣカードから取出した鍵を付加した暗号鍵設定命令を前記通信手段を介して送信することにより、該鍵を前記他方のＩＣカード内に記憶せしめる暗号鍵設定手段とを具備している。

【 0 0 1 7 】

また、本発明のＩＣカード端末装置は、２つのＩＣカードとの間でデータを通信する通信手段と、前記２つのＩＣカードに対し、第１の鍵を暗号化あるいは復号化するための第２の鍵を付加した鍵設定命令を前記通信手段を介して送信することにより、該第２の鍵を前記２つのＩＣカード内にそれぞれ記憶せしめる第１の鍵設定手段と、この第１の鍵設定手段による前記第２の鍵の設定が正常に終了したことを確認する確認手段と、この確認手段により第２の鍵の設定が正常に終了したことが確認されると、前記２つのＩＣカードのうち一方のＩＣカードに対

し鍵生成命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内においてデータを暗号化あるいは復号化するための前記第１の鍵を生成せしめる鍵生成手段と、この鍵生成手段により第１の鍵を生成させた前記一方のＩＣカードに対し鍵取出命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内で生成された第１の鍵を前記通信手段を介して取出す鍵取出手段と、前記２つのＩＣカードのうち他方のＩＣカードに対し前記鍵取出手段により前記一方のＩＣカードから取出した第１の鍵を付加した暗号鍵設定命令を前記通信手段を介して送信することにより、該第１の鍵を前記他方のＩＣカード内に記憶せしめる第２の鍵設定手段とを具備している。

【 0 0 1 8 】

また、本発明のＩＣカード複製方法は、少なくともデータを暗号化あるいは復号化するための鍵が記憶されている被複製用の第１のＩＣカードと、複製用の第２のＩＣカードと、これら第１、第２のＩＣカードを取扱う端末装置とを有し、前記端末装置から前記第１のＩＣカードに対し鍵取出命令を送信する第１のステップと、前記第１のＩＣカードにおいて、前記端末装置から送信された鍵取出命令を受信し、前記鍵を前記端末装置に対し送信する第２のステップと、前記端末装置において、前記第１のＩＣカードから送信された鍵を受信し、この受信した鍵を付加した暗号鍵設定命令を前記第２のＩＣカードに対し送信する第３のステップと、前記第２のＩＣカードにおいて、前記端末装置から送信された暗号鍵設定命令を受信し、その暗号鍵設定命令に付加された鍵を記憶する第４のステップとを具備している。

【 0 0 1 9 】

また、本発明のＩＣカード複製方法は、少なくともデータを暗号化あるいは復号化するための第１の鍵が記憶されている被複製用の第１のＩＣカードと、複製用の第２のＩＣカードと、これら第１、第２のＩＣカードを取扱う端末装置とを有し、前記端末装置から前記第１、第２のＩＣカードに対し、前記第１の鍵を暗号化あるいは復号化するための第２の鍵を付加した鍵設定命令を送信する第１のステップと、前記第１、第２のＩＣカードにおいて、前記端末装置から送信された鍵設定命令を受信し、その鍵設定命令に付加された第２の鍵をそれぞれ記憶す

る第2のステップと、前記端末装置から前記第1のICカードに対し鍵取出命令を送信する第3のステップと、前記第1のICカードにおいて、前記端末装置から送信された鍵取出命令を受信し、前記第2のステップで記憶された第2の鍵により前記第1の鍵を暗号化し、この暗号化した第1の鍵を前記端末装置に対し送信する第4のステップと、前記端末装置において、前記第1のICカードから送信された暗号化された第1の鍵を受信し、この受信した暗号化された第1の鍵を付加した暗号鍵設定命令を前記第2のICカードに対し送信する第5のステップと、前記第2のICカードにおいて、前記端末装置から送信された暗号鍵設定命令を受信し、その暗号鍵設定命令に付加された暗号化された第1の鍵を前記第2のステップで記憶された第2の鍵により復号化し、この復号化した第1の鍵を記憶する第6のステップとを具備している。

【0020】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。

【0021】

図1は、本発明の実施の形態に係るICカード発行システムの構成例を概略的に示すものである。図1において、このICカード発行システムは、端末装置200およびカード発行装置210を備えていて、両者はケーブル205を介して接続されている。端末装置200は、たとえば、パーソナルコンピュータ（PC）であり、端末本体201、補助記憶装置としてのハードディスク装置（HDD）202、入力装置としてのキーボード203、および、ディスプレイ204を備えている。

【0022】

端末本体201は、演算部としてのCPU（セントラル・プロセッシング・ユニット）201a、および、主記憶装置としてのメモリ201bを備えている。CPU201aは、本発明のポイントである鍵設定処理を制御する。また、端末本体201は、ハードディスク装置202、キーボード203、および、ディスプレイ204とそれぞれ接続されている。

【0023】

ハードディスク装置 2 0 2 には、データ項目定義ファイル F 1 1、磁気エンコード用データベースファイル F 1 2、個人データベースファイル F 1 3、共通データベースファイル F 1 4、命令コードデータベースファイル F 1 5、および、印刷デザイン定義ファイル F 1 6 などが格納されている。

【 0 0 2 4 】

カード発行装置 2 1 0 は、カードリーダー・ライター 2 0 6、カード印刷機 2 0 7、磁気エンコーダ 2 0 8、カード供給部 2 1 1、スタッカ 2 1 2 を備えていて、カード供給部 2 1 1 にセットされた発行すべき IC カード 1 0 0 を 1 枚ずつ取込み、取込んだ IC カード 1 0 0 を該カード発行装置 2 1 0 内を経由させた後、カードスタッカ 2 1 2 へ排出するようになっている。

【 0 0 2 5 】

IC カード 1 0 0 は、たとえば、図 2 に示すように、コンタクト部 1 0 5、IC チップ 1 0 6、および、磁気ストライプ部 1 0 7 を備えている。IC チップ 1 0 6 は、制御素子 1 0 1、データメモリ 1 0 2、ワーキングメモリ 1 0 3、および、プログラムメモリ 1 0 4 を備えている。コンタクト部 1 0 5 および IC チップ 1 0 6 は一体的にモジュール化され、IC カード本体に埋設されている。

【 0 0 2 6 】

制御素子 1 0 1 は、たとえば、CPU である。この制御素子 1 0 1 は、本発明のポイントである鍵設定処理、鍵生成処理、鍵暗号化処理などを実行する。データメモリ 1 0 2 は、記憶内容が消去可能な不揮発性のメモリであり、たとえば、EEPROM (electrically erasable and programmable ROM) である。ワーキングメモリ 1 0 3 は、制御素子 1 0 1 の処理データなどを一時的に格納するメモリであり、たとえば、RAM (random access memory) である。プログラムメモリ 1 0 4 は、制御素子 1 0 1 のプログラムなどを記憶するメモリであり、たとえば、マスク ROM (read only memory) である。コンタクト部 1 0 5 は、カード発行装置 2 1 0 のカードリーダー・ライター 2 0 6 と電氣的に接触する部分であり、このコンタクト部 1 0 5 およびカードリーダー・ライター 2 0 6 を介してカード発行装置 2 1 0 と IC カード 1 0 0 との間で各種データ交換が行なわれる。

【 0 0 2 7 】

カード発行装置 2 1 0 のカードリーダー・ライタ 2 0 6 は、IC カード 1 0 0 のコンタクト部 1 0 5 を介して IC カード 1 0 0 との間で各種データ交換を行なう。また、カードリーダー・ライタ 2 0 6 は、IC カード 1 0 0 の磁気ストライプ部 1 0 7 に対して各種データを磁気記録したり、磁気ストライプ部 1 0 7 に磁気記録された各種データを読み出したりもする。

【 0 0 2 8 】

カード発行装置 2 1 0 は、以下に示す [1] ~ [4] の各機能をそれぞれ備えている。

【 0 0 2 9 】

[1] 端末装置 2 0 0 からカード発行装置 2 1 0 に送られた命令データを IC カード 1 0 0 のコンタクト部 1 0 5 を介して制御素子 1 0 1 に送信する機能（カードリーダー・ライタ 2 0 6 ）。

【 0 0 3 0 】

[2] IC カード 1 0 0 の制御素子 1 0 1 から送られた応答をコンタクト部 1 0 5 を介してカード発行装置 2 1 0 から端末装置 2 0 0 に送信する機能（カードリーダー・ライタ 2 0 6 ）。

【 0 0 3 1 】

[3] 端末装置 2 0 0 からカード発行装置 2 1 0 に送られた印刷データを IC カード 1 0 0 の表面に印刷する機能（カード印刷機 2 0 7 ）。

【 0 0 3 2 】

[4] 端末装置 2 0 0 からカード発行装置 2 1 0 に送られた磁気エンコードデータを IC カード 1 0 0 の磁気ストライプ部 1 0 7 に磁気記録する機能（磁気エンコーダ 2 0 8 ）。

【 0 0 3 3 】

図 3 は、カード発行装置 2 1 0、端末装置 2 0 0 側から送信された命令（鍵設定命令、鍵生成命令、鍵取出命令など）に対して IC カード 1 0 0 側から出力される出力情報（レスポンス）のフォーマット例を示すものである。なお、鍵設定命令、鍵生成命令、鍵取出命令の各機能については後に説明する。

【 0 0 3 4 】

図 3 (a) に示す第 1 のフォーマットは、ステータスコードを出力情報として含む。このステータスコードは、カード発行装置 2 1 0 側から送信された命令の実行結果を示す。

【 0 0 3 5 】

図 3 (b) に示す第 2 のフォーマットは、データ部およびステータスコードを出力情報として含む。このステータスコードは、上記同様にカード発行装置 2 1 0 側から送信された命令の実行結果を示す。なお、データ部については後で詳細に説明する。

【 0 0 3 6 】

図 4 は、IC カード 1 0 0 のデータメモリ 1 0 2 におけるファイル構造の一例を示すものである。

【 0 0 3 7 】

図 4 (a) は、A さんが所持する IC カード 1 0 0 a (IC カード a と表記することもある) のデータメモリ 1 0 2 におけるファイル構造を示しており、メインファイル (MF) を中心として、このメインファイル (MF) に複数のサブファイル (IEF 1、IEF 2、IEF 3、IEF 4、IEF 5、IEF 6、WEF 1、WEF 2) がぶら下がる構造になっている。サブファイル (IEF 1、IEF 2、IEF 3、IEF 4、IEF 5、IEF 6) は、鍵格納部として機能し、サブファイル (IEF 1) には鍵 1 (A) が格納され、サブファイル (IEF 2) には鍵 2 (A) が格納され、サブファイル (IEF 3) には鍵 3 (A) が格納され、サブファイル (IEF 4) には復号化用鍵 A が格納され、サブファイル (IEF 5) には暗号化用鍵 A が格納され、サブファイル (IEF 6) には暗号化用鍵 B が格納される。これら、鍵 1 (A)、鍵 2 (A)、鍵 3 (A) を合わせて鍵群 (第 2 の鍵) と称し、復号化用鍵 (A)、暗号化用鍵 (A)、暗号化用鍵 (B) をシステムで利用する本鍵 (第 1 の鍵) とする。また、サブファイル (WEF 1) には A さんの会員番号 (A) が格納され、サブファイル (WEF 2) には該カードの有効期限 (A) が格納される。

【 0 0 3 8 】

図 4 (b) は、A さんとは異なる B さんが所持する IC カード 1 0 0 b (IC

カードbと表記することもある)のデータメモリ102におけるファイル構造を示しており、上記同様、メインファイル(MF)を中心として、このメインファイル(MF)に複数のサブファイル(IEF1、IEF2、IEF3、IEF4、IEF5、IEF6、WEF1、WEF2)がぶら下がる構造になっている。サブファイル(IEF1)には鍵1(B)が格納され、サブファイル(IEF2)には鍵2(B)が格納され、サブファイル(IEF3)には鍵3(B)が格納され、サブファイル(IEF4)には復号化用鍵(B)が格納され、サブファイル(IEF5)には暗号化用鍵(B)が格納され、サブファイル(IEF6)には暗号化用鍵(A)が格納される。これら、鍵1(B)、鍵2(B)、鍵3(B)を合わせて鍵群(第2の鍵)と称し、復号化用鍵(B)、暗号化用鍵(B)、暗号化用鍵(A)をシステムで利用する本鍵(第1の鍵)とする。また、サブファイル(WEF1)にはBさんの会員番号(B)が格納され、サブファイル(WEF2)には該カードの有効期限(B)が格納される。

【0039】

ICカード100のICチップ106内では、本鍵を利用してデータの隠蔽とデータの正当性の確認処理が行なわれる。ICチップ106内では、鍵群を利用して本鍵の暗号化が行なわれる。本鍵は、セキュリティを高めるため、ICチップ106内で生成されるものである。鍵群は、本鍵を暗号化するもので、カード発行時にカード発行装置210で生成される鍵設定命令、後述する個人端末装置で生成される鍵設定命令、あるいは、特殊鍵設定命令により設定されるものであり、正しい暗号化を実行させるためには正しい鍵群が設定されなければならない。

【0040】

図5は、ICカード100内の鍵を利用するシステム例を示すものである。

【0041】

図5において、ICカード端末装置としての個人端末装置300(個人端末装置(A)と表記することもある)はAさんが所持し、同じく個人端末装置400(個人端末装置(B)と表記することもある)はBさんが所持し、これら個人端末装置300と個人端末装置400とはネットワークやLANなどの通信回線5

00を介して接続されていて、両者の間で各種データの交換や各種電子データファイルの交換が行なわれるようになっている。

【0042】

個人端末装置300は、たとえば、パーソナルコンピュータ（PC）であり、端末本体301、補助記憶装置としてのハードディスク装置（HDD）302、入力装置としてのキーボード303、および、ディスプレイ304を備えている。

【0043】

端末本体301は、演算部としてのCPU301a、および、主記憶装置としてのメモリ301bを備えている。CPU301aは、本発明のポイントである鍵設定処理を制御する。また、端末本体301は、ハードディスク装置302、キーボード303、および、ディスプレイ304、および、カードリーダー・ライタ306（カードリーダー・ライタAと表記することもある）とそれぞれ接続されている。ハードディスク装置302には、暗号化用鍵Aで暗号化された機密情報である電子データファイルF21、F22、F23などが格納されている。なお、電子データファイルは、たとえば、電子メール、文書ファイル、プログラムソースなどである。

【0044】

個人端末装置300は、カードリーダー・ライタ306を介してICカード100aとの間で各種データの交換を行なう。

【0045】

個人端末装置400も上記同様に構成されている。すなわち、個人端末装置400は、たとえば、パーソナルコンピュータ（PC）であり、端末本体401、補助記憶装置としてのハードディスク装置（HDD）402、入力装置としてのキーボード403、および、ディスプレイ404を備えている。

【0046】

端末本体401は、演算部としてのCPU401a、および、主記憶装置としてのメモリ401bを備えている。CPU401aは、本発明のポイントである鍵設定処理を制御する。また、端末本体401は、ハードディスク装置402、

キーボード 4 0 3、および、ディスプレイ 4 0 4、および、カードリーダー・ライタ 4 0 6（カードリーダー・ライタ B と表記することもある）とそれぞれ接続されている。ハードディスク装置 4 0 2 には、暗号化用鍵 B で暗号化された機密情報である電子データファイル F 3 1、F 3 2、F 3 3 などが格納されている。

【 0 0 4 7 】

個人端末装置 4 0 0 は、カードリーダー・ライタ 4 0 6 を介して I C カード 1 0 0 b との間で各種データの交換を行なう。

【 0 0 4 8 】

個人端末装置 3 0 0 と個人端末装置 4 0 0 とは、上記したように、ネットワークや L A N などの通信回線 5 0 0 を介して各種データの交換や各種電子データファイルの交換が行なわれる。その場合、セキュリティを高めるために、たとえば、個人端末装置 4 0 0 から個人端末装置 3 0 0 に電子データファイルを送る場合、個人端末装置 4 0 0 は、まず、カードリーダー・ライタ 4 0 6 を介して I C カード 1 0 0 b に対して、たとえば、電子データファイル 1（電子データファイル F 3 1）を付加した暗号化用鍵（A）での暗号化命令を送信する。

【 0 0 4 9 】

I C カード 1 0 0 b のコンタクト部 1 0 5 で受信された暗号化用鍵（A）での暗号化命令は、制御素子 1 0 1 で解読される。この解読の際、暗号化用鍵（A）での暗号化命令であることが判明し、この解読結果に基づき、暗号化命令に付加された電子データファイル 1 を復号化用鍵 B で復号化を行ない、その後、暗号化用鍵 A を使用して暗号化を行ない、暗号化命令に対するレスポンスとして、正常終了情報および暗号化結果がコンタクト部 1 0 5 からカードリーダー・ライタ 4 0 6 を介して個人端末装置 4 0 0 に送信される。

【 0 0 5 0 】

個人端末装置 4 0 0 は、I C カード 1 0 0 b からのレスポンス情報（暗号化用鍵 A で暗号化された電子データファイル 1）を個人端末装置 3 0 0 に送る。個人端末装置 3 0 0 は、受取った情報（暗号化用鍵 A で暗号化された電子データファイル 1）をハードディスク装置 3 0 2 の電子データファイル F 2 1 に保存する。受取った情報（暗号化用鍵 A で暗号化された電子データファイル 1）を閲覧する

場合、端末装置 3 0 0 は、まず、カードリーダー・ライタ 3 0 6 を介して I C カード 1 0 0 a に対して、暗号化用鍵 A で暗号化された電子データファイル 1（電子データファイル F 2 1）を付加した復号化用鍵（A）での復号化命令を送信する。

【 0 0 5 1 】

I C カード 1 0 0 a のコンタクト部 1 0 5 で受信された復号化用鍵（A）での復号化命令は、制御素子 1 0 1 で解読される。この解読の際、復号化用鍵（A）での復号化命令であることが判明し、この解読結果に基づき、復号化命令に付加された電子データファイル 1 を復号化鍵用 A で復号化を行ない、復号化命令に対するレスポンスとして、正常終了情報および復号化結果がコンタクト部 1 0 5 からカードリーダー・ライタ 3 0 6 を介して個人端末装置 3 0 0 に送信される。

【 0 0 5 2 】

このように、I C カード内の復号化用鍵を利用して、I C カード内でのみ復号化を行なうためセキュリティが高いが、たとえば、I C カードの破損などで復号化用鍵を失った場合は、個人端末装置 3 0 0 のハードディスク装置 3 0 2 に保存されている電子データファイルを復号化することが不可能となる。また、個人端末装置 4 0 0 から送られてくるデータを復号化することも不可能となる。

【 0 0 5 3 】

そこで、本発明では、以下に詳細を説明するバックアップカード（バックアップ用の I C カードと表記することもある）の作成処理にしたがい、カード発行装置 2 1 0 により I C カード 1 0 0 に対して、本カード（正規の I C カード）の作成およびバックアップカード（正規の I C カードの複製カード）の作成を行ない、個人端末装置 3 0 0 または 4 0 0 において、本カード内で暗号化用鍵および復号化用鍵の生成を行ない、即時にバックアップカードを作成することで、本カードの破損時にバックアップカードを使うことにより、電子データファイルの復号化を行ない、新しい I C カードで暗号化を行なうことにより、電子データファイルが復号化不可能となることを防止するものである。

【 0 0 5 4 】

まず、図 6 ないし図 1 0 を参照して I C カード発行システムの端末装置 2 0

0で生成される命令データの生成方法について説明する。

【0055】

端末装置200のハードディスク装置202内に保管されている個人データベースファイルF13は、たとえば、図6に示すように、漢字氏名（項目1）、漢字住所（項目2）、カナ名字（項目3）、会員番号（項目4）、有効期限（項目5）、パスワード（項目6）、鍵1（項目7）などの個別データを1レコードとしたレコード群（個別データ群）から構成されている。

【0056】

また、ハードディスク装置202内に保管されている本カード用の命令コードデータベースファイルF15は、ICカード100のICチップ106内の制御素子101に対して条件設定を行ったり、付加データをデータメモリ102に書込ませる働きをする命令コードなどから構成される。たとえば、図7に示すように、命令コード欄、付加データ欄、IC出力情報欄が用意されており、図7の例では、たとえば、「命令コード18」の付加データは「個人データベースファイルの項目6」が定義されて、IC出力情報は「9000」と比較すると定義され、「命令コード25」の付加データは「個人データベースファイルの項目5」が定義されて、IC出力情報は「9000」と比較すると定義されている。

【0057】

端末装置200は、命令コードデータベースと個人データベースとから、たとえば、図10に示すように、命令コード19に付加データとして個人データベースファイルの項目7のデータ「49 83..6c 44 78」が付加された命令データを生成する。

【0058】

たとえば、復号化用鍵取出し・設定命令用鍵群の鍵1は次のように設定する。端末装置200は、ハードディスク装置202内に格納されている命令コードデータベースファイル（図7参照）の命令コード19と、個人データベースファイル（図6参照）の項目7とから命令データを生成し、カードリーダー・ライター206を介してICカード100のICチップ106に送ることにより、鍵1を設定する。この命令コード19を鍵設定命令と称する。

【0059】

ICカード100のICチップ106内での動作をさらに詳細に説明すると、カードリーダー・ライタ206からICカード100のコンタクト部105に対して、鍵1が付加された鍵設定命令が送信される。コンタクト部105で受信された鍵設定命令は、制御素子101で解読される。この解読の際、鍵1の設定命令であることが判明し、この解読結果に基づき鍵1がデータメモリ102のサブファイル（IEF1）に設定（記憶）される。そして、鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部105からカードリーダー・ライタ206に送信される。すなわち、正常終了情報が端末本体201に通知されることになる。

【0060】

バックアップカード用の命令コードデータベースファイルは、本カード用命令コードデータベースファイルと同様に、ICカード100のICチップ106内の制御素子101に対して条件設定を行ったり、付加データをデータメモリ102に書込ませる働きをする命令コードなどから構成される。たとえば、図8に示すように、命令コード欄、付加データ欄、IC出力情報欄が用意されており、図8の例では、たとえば、「命令コード18」の付加データは「個人データベースファイルの項目6」が定義されている。

【0061】

バックアップカードは、たとえば、図9に示すように、本カードとしての機能を果たすための必須情報である会員番号や有効期限の情報がないファイル構造となっている。したがって、バックアップカード用の命令コードデータベースファイルは、本カード用の命令コードデータベースファイルと異なり、鍵1の設定情報以降の命令コードは定義されない。

【0062】

次に、本カードおよびバックアップカードの発行処理について、図11に示すフローチャートを参照して説明する。

【0063】

まず、カード供給部211からICカード100を取込み（S101）、その

後、本カード用の命令コードデータベースファイルF 1 5に基づき命令コードを生成して（S 1 0 2）、それをICカード1 0 0に送る（S 1 0 3）。

【 0 0 6 4 】

次に、本カード用の印刷デザイン定義ファイルF 1 6に基づきカード表面の印刷データを生成し、この生成した印刷データをカード印刷機2 0 7へ送ることにより、ICカード1 0 0の表面に印刷を行なう（S 1 0 4）。

【 0 0 6 5 】

次に、本カード用の磁気エンコード用データベースファイルF 1 2に基づき磁気記録データを生成し、この生成した磁気記録データを磁気エンコーダ2 0 8へ送ることにより、ICカード1 0 0磁気ストライプ部1 0 7に磁気記録を行なう（S 1 0 5）。

【 0 0 6 6 】

次に、本カードの発行処理が正常に終了したかを確認し（S 1 0 6）、正常に終了した場合、該ICカード1 0 0をスタッカ2 1 2に排出する（S 1 0 7）。スタッカ2 1 2に排出されたICカード1 0 0は本カードとして発行されたICカードである。

【 0 0 6 7 】

スタッカ2 1 2に本カードを排出した後、カード供給部2 1 1から2枚目のICカード1 0 0を取込み、その後、バックアップカード用の命令コードデータベースファイルF 1 5に基づき命令コードを生成して（S 1 0 8）、それをICカード1 0 0に送る（S 1 0 9）。

【 0 0 6 8 】

次に、バックアップカード用の印刷デザイン定義ファイルF 1 6に基づきカード表面の印刷データを生成し、この生成した印刷データをカード印刷機2 0 7へ送ることにより、ICカード1 0 0の表面に印刷を行なう（S 1 1 0）。

【 0 0 6 9 】

次に、バックアップカード用の磁気エンコード用データベースファイルF 1 2に基づき磁気記録データを生成し、この生成した磁気記録データを磁気エンコーダ2 0 8へ送ることにより、ICカード1 0 0の磁気ストライプ部1 0 7に磁気

記録を行なう（S 1 1 1）。

【0 0 7 0】

次に、バックアップカードの発行処理が正常に終了したかを確認し（S 1 1 2）、正常に終了した場合、該 I C カード 1 0 0 をスタッカ 2 1 2 に排出する（S 1 1 3）。スタッカ 2 1 2 に排出された I C カード 1 0 0 はバックアップカードとして発行された I C カードである。

【0 0 7 1】

なお、ステップ S 1 0 6、S 1 1 2 において、カードの発行処理が正常に終了しなかった場合、該 I C カード 1 0 0 を図示しないリジェクト部に排出する（S 1 1 4）。

【0 0 7 2】

このようにして、本カードおよびバックアップカードの発行処理が行なわれるものであり、発行処理終了直後（カード製造者からの出荷状態）の両カードにおけるデータメモリ 1 0 2 の内部の状態を図 1 2 に模式的に示す。上記した発行処理により、図に網掛けしたファイル（I E F 1、W E F 1、W E F 2）に所定のデータが設定（記憶）され、網掛けのない他のファイル（I E F 2、I E F 3、I E F 4、I E F 5、I E F 6）はデータ未設定の状態である。

【0 0 7 3】

次に、上記したように発行された本カードに暗号化用鍵および復号化用鍵を生成させ、バックアップカードに復号化用鍵を設定する処理について説明する。なお、以下の説明では個人端末装置 3 0 0 を用いて行なう場合について述べるが、個人端末装置 4 0 0 を用いても同様に行なえる。

【0 0 7 4】

まず、本カードに暗号化用鍵および復号化用鍵を生成させ、バックアップカードに復号化用鍵を設定するシステムの構成について図 1 3 を参照して説明する。図 1 3 において、個人端末装置 3 0 0 には、本カード用のカードリーダー・ライタ 3 0 6 a と共にバックアップカード用のカードリーダー・ライタ 3 0 6 b が接続されており、カードリーダー・ライタ 3 0 6 a には前記のように発行された本カード 1 0 0 c（I C カード a に対応、本カード a と表記することもある）が挿入され

、カードリーダー・ライタ 3 0 6 b には前記のように発行されたバックアップカード 1 0 0 d (バックアップカード a と表記することもある) が挿入される。

【 0 0 7 5 】

個人端末装置 3 0 0 のディスプレイ 3 0 4 には、図 1 4 に示すような鍵入力画面が表示される。この鍵入力画面には、復号化用鍵取出し・設定命令用鍵群のうち、前述の発行処理で設定を行なわなかった鍵を入力するエリア、および、鍵設定を行なうために必要な照合用パスワードの入力エリア、鍵入力の終了を指示する入力終了釦、処理を中断するための終了釦がそれぞれ表示されている。

【 0 0 7 6 】

設定対象となる鍵群 (鍵 2、鍵 3) は、オペレータによるキーボード 3 0 3 の操作により端末本体 3 0 1 に入力される。全ての鍵 (鍵 2、鍵 3) とパスワードの入力が終了し、入力終了釦により入力終了が指示されると、本カード 1 0 0 c およびバックアップカード 1 0 0 d への鍵の設定、本カード 1 0 0 c での暗号化用鍵、復号化用鍵の生成、本カード 1 0 0 c から復号化用鍵の取出し、バックアップカード 1 0 0 d への復号化用鍵の設定が開始される。

【 0 0 7 7 】

次に、本カード 1 0 0 c およびバックアップカード 1 0 0 d への鍵の設定、本カード 1 0 0 c での暗号化用鍵および復号化用鍵の生成、本カード 1 0 0 c からの復号化用鍵の取出し、バックアップカード 1 0 0 d への復号化用鍵の設定を行なう処理について、図 1 5 に示すフローチャートを参照して説明する。

【 0 0 7 8 】

鍵の設定は、鍵設定命令により実行される。すなわち、カードリーダー・ライタ 3 0 6 a を介して本カード 1 0 0 c のコンタクト部 1 0 5 に対して、鍵 2 の鍵入力エリアに入力された鍵 2 が付加された鍵設定命令データが送信される (S 2 0 1)。本カード 1 0 0 c のコンタクト部 1 0 5 で受信された受信データは、制御素子 1 0 1 で解読される。この解読の際、受信データは鍵 2 の設定命令であることが判明すると、この解読結果に基づき鍵 2 がデータメモリ 1 0 2 のサブファイル (I E F 2) に設定 (記憶) される (S 2 0 1 a)。そして、鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部 1 0 5 からカードリーダー・

ライター 3 0 6 a に送信される。すなわち、正常終了情報が端末本体 3 0 1 に通知されることになる。

【 0 0 7 9 】

次に、カードリーダー・ライター 3 0 6 b を介してバックアップカード 1 0 0 d のコンタクト部 1 0 5 に対して、鍵 2 の鍵入力エリアに入力された鍵 2 が付加された鍵設定命令が送信され (S 2 0 2) 、上記同様に鍵 2 がバックアップカード 1 0 0 d のデータメモリ 1 0 2 のサブファイル (I E F 2) に設定 (記憶) される (S 2 0 2 a) 。そして、鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部 1 0 5 からカードリーダー・ライター 3 0 6 b に送信される。すなわち、正常終了情報が端末本体 3 0 1 に通知されることになる。

【 0 0 8 0 】

この後、カードリーダー・ライター 3 0 6 a を介して本カード 1 0 0 c のコンタクト部 1 0 5 に対して、鍵 3 の鍵入力エリアに入力された鍵 3 が付加された鍵設定命令が送信され (S 2 0 3) 、上記同様に鍵 3 が本カード 1 0 0 c のデータメモリ 1 0 2 のサブファイル (I E F 3) に設定 (記憶) される (S 2 0 3 a) 。そして、鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部 1 0 5 からカードリーダー・ライター 3 0 6 a に送信される。すなわち、正常終了情報が端末本体 3 0 1 に通知されることになる。

【 0 0 8 1 】

次に、カードリーダー・ライター 3 0 6 b を介してバックアップカード 1 0 0 d のコンタクト部 1 0 5 に対して、鍵 3 の鍵入力エリアに入力された鍵 3 が付加された鍵設定命令が送信され (S 2 0 4) 、上記同様に鍵 3 がバックアップカード 1 0 0 d のデータメモリ 1 0 2 のサブファイル (I E F 3) に設定される (S 2 0 4 a) 。そして、鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部 1 0 5 からカードリーダー・ライター 3 0 6 b に送信される。すなわち、正常終了情報が端末本体 3 0 1 に通知されることになる。

【 0 0 8 2 】

本カード 1 0 0 c での暗号化用鍵、復号化用鍵の生成は、暗号化用鍵・復号化用鍵生成命令により実行される。すなわち、カードリーダー・ライター 3 0 6 a を介

して本カード100cのコンタクト部105に対して、暗号化用鍵・復号化用鍵生成命令データが送信される(S205)。コンタクト部105で受信された受信データは、制御素子101で解読される。この解読の際、受信データは暗号化用鍵・復号化用鍵生成命令であることが判明すると、この解読結果に基づき暗号化用鍵・復号化用鍵が生成され、データメモリ102のサブファイル(IEF4、IEF5)に設定(記憶)される(S205a)。そして、暗号化用鍵・復号化用鍵生成命令に対するレスポンスとして、正常終了情報がコンタクト部105からカードリーダー・ライタ306aに送信される。すなわち、正常終了情報が端末本体301に通知されることになる。

【0083】

本カード100cから復号化用鍵の取出しは復号化用鍵取出命令により実行される。すなわち、カードリーダー・ライタ306aを介して本カード100cのコンタクト部105に対して、復号化用鍵取出命令データが送信される(S206)。コンタクト部105で受信された受信データは、制御素子101で解読される。この解読の際、受信データは復号化用鍵取出命令であることが判明すると、この解読結果に基づき、データメモリ102のサブファイル(IEF4)に設定されている復号化用鍵を鍵群(鍵1、鍵2、鍵3)で暗号化した結果と正常終了情報が、復号化用鍵取出命令に対するレスポンスとして、コンタクト部105からカードリーダー・ライタ306aに送信される(S206a、S207)。すなわち、正常終了情報と鍵群により暗号化された復号化用鍵が端末本体301に通知されることになる。

【0084】

バックアップカード100dへの復号化用鍵の設定は、上記で通知された鍵群により暗号化された復号化用鍵が付加された復号化用鍵設定命令により実行される。すなわち、カードリーダー・ライタ306bを介してバックアップカード100dのコンタクト部105に対して、復号化用鍵設定命令データが送信される(S208)。コンタクト部105で受信された受信データは、制御素子101で解読される。この解読の際、受信データは復号化用鍵設定命令であることが判明すると、この解読結果に基づき、データメモリ102のサブファイル(IEF1

、 I E F 2、 I E F 3）に設定されている鍵群（鍵 1、鍵 2、鍵 3）で、復号化用鍵設定命令に付加された暗号化された復号化用鍵を復号化し、データメモリ 1 0 2 のサブファイル（I E F 4）に設定される（S 2 0 8 a）。そして、復号化用鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部 1 0 5 からカードリーダー・ライター 3 0 6 b に送信される。すなわち、正常終了情報が端末本体 3 0 1 に通知されることになる。

【 0 0 8 5 】

このようにして、本カード 1 0 0 c に暗号化用鍵および復号化用鍵を生成させ、バックアップカード 1 0 0 d に復号化用鍵を設定するものであり、処理終了直後（ユーザ使用開始前状態）の両カードにおけるデータメモリ 1 0 2 の内部の状態を図 1 6 に模式的に示す。上記した処理により、図に縦破線、横破線、格子柄を付したファイル（I E F 2、I E F 3、I E F 4、I E F 5）に所定のデータが設定（記憶）され、何も付されていない他のファイル（I E F 6、I E F 5）はデータ未設定の状態である。

【 0 0 8 6 】

上記で説明した本カード 1 0 0 c の作成およびバックアップカード 1 0 0 d の作成の処理の模様を模式図で表わすと、図 1 7 に示すようになる。

【 0 0 8 7 】

次に、このように作成された本カード 1 0 0 c が破損し、個人端末装置 3 0 0 の電子データファイルをバックアップカード 1 0 0 d で復号化し、新しい本カードで暗号化する処理について説明する。なお、以下の説明では個人端末装置 3 0 0 を用いて行なう場合について述べるが、個人端末装置 4 0 0 を用いても同様に行なえる。

【 0 0 8 8 】

個人端末装置 3 0 0 には、図 1 3 を用いて先に説明したように、新しい本カード挿入用のカードリーダー・ライター 3 0 6 a と共にバックアップカード挿入用のカードリーダー・ライター 3 0 6 b が接続されており、カードリーダー・ライター 3 0 6 a には新たに作成された本カード 1 0 0 c が挿入され、カードリーダー・ライター 3 0 6 b にはバックアップカード 1 0 0 d が挿入される。

【 0 0 8 9 】

個人端末装置 3 0 0 のディスプレイ 3 0 4 には、たとえば、図 1 8 に示すようなファイル名入力画面が表示されている。このファイル名入力画面には、新しいカードで暗号化を行なうために必要な照合用パスワードの入力エリア、バックアップカードで復号化を行なうために必要な照合用パスワードの入力エリア、破損した旧い本カード 1 0 0 c の暗号化用鍵で暗号化された電子データファイル名を入力する追加釐、電子データファイル名を表示するエリア、ファイル名入力の終了を指示する入力終了釐、処理を中断するための終了釐が表示されている。

【 0 0 9 0 】

オペレータによるキーボード 3 0 3 の操作により、破損した旧い本カード 1 0 0 c の暗号化用鍵で暗号化された電子データファイル名の入力と、パスワードの入力が終了し、入力終了釐により入力終了が指示されると、バックアップカード 1 0 0 d での電子データファイルの復号化処理、および、新しい本カード 1 0 0 c での電子データファイルの暗号化処理が開始される。

【 0 0 9 1 】

以下、バックアップカード 1 0 0 d での電子データファイルの復号化処理、および、新しい本カード 1 0 0 c での電子データファイルの暗号化処理について、図 1 9 に示すフローチャートを参照して説明する。

【 0 0 9 2 】

まず、入力されたバックアップカードで復号化を行なうために必要な照合用パスワードを基にバックアップカードで復号化を行なうために必要な照合の命令データが作成され、カードリーダー・ライター 3 0 6 b を介してバックアップカード 1 0 0 d に送信される（S 3 0 1）。次に、新しいカードで暗号化を行なうために必要な照合用パスワードを基に新しいカードで暗号化を行なうために必要な照合の命令データが作成され、カードリーダー・ライター 3 0 6 a を介して新しい本カード 1 0 0 c に送信される（S 3 0 2）。

【 0 0 9 3 】

電子データファイルの復号化処理は、復号化命令により実行される。すなわち、カードリーダー・ライター 3 0 6 b を介してバックアップカード 1 0 0 d のコンタ

クト部 1 0 5 に対して、ファイル名入力エリアに入力された電子データファイルが付加された復号化命令が送信される (S 3 0 3、S 3 0 4)。

【0 0 9 4】

バックアップカード 1 0 0 d のコンタクト部 1 0 5 で受信された復号化命令は、バックアップカード 1 0 0 d の制御素子 1 0 1 で解読される。この解読の際、復号化命令であることが判明し、この解読結果に基づき、制御素子 1 0 1 は、データメモリ 1 0 2 のサブファイル (I E F 4) に設定されている復号化用鍵で復号化命令に付加されてきた電子データファイルを復号化し (S 3 0 4 a)、その復号化結果と正常終了情報がコンタクト部 1 0 5 からカードリーダー・ライター 3 0 6 b に送信する (S 3 0 5)。

【0 0 9 5】

電子データファイルの暗号化処理は、暗号化命令により実行される。すなわち、カードリーダー・ライター 3 0 6 a を介して新しい本カード 1 0 0 c のコンタクト部 1 0 5 に対して、上記で通知された復号化された電子データファイルが付加された暗号化命令が送信される (S 3 0 6)。

【0 0 9 6】

新しい本カード 1 0 0 c のコンタクト部 1 0 5 で受信された暗号化命令は、新しい本カード 1 0 0 c の制御素子 1 0 1 で解読される。この解読の際、暗号化命令であることが判明し、この解読結果に基づき、制御素子 1 0 1 は、データメモリ 1 0 2 のサブファイル (I E F 5) に設定されている暗号化用鍵で暗号化命令に付加されてきた電子データファイルを暗号化し (S 3 0 6 a)、その暗号化結果と正常終了情報がコンタクト部 1 0 5 からカードリーダー・ライター 3 0 6 a を介して端末本体 3 0 1 に送信する (S 3 0 7)。

【0 0 9 7】

端末本体 3 0 1 は、新しい本カード 1 0 0 c からの暗号化用鍵で暗号化された電子データファイルをハードディスク装置 3 0 2 に格納する (S 3 0 8)。次に、新しい本カード 1 0 0 c から受取った暗号化された電子データファイルが最後の電子データファイルか否かを判断し (S 3 0 9)、最後でなければステップ S 3 0 3 からの動作を繰り返し、最後の電子データファイルになったところで処理

を終了する。

【0098】

このように、上記実施の形態によれば、ＩＣカード内で生成された復号化用鍵、暗号化用鍵を外部へ取出す際、該ＩＣカード内に設定された別の複数の鍵で暗号化してから外部へ取出すことにより、安全に外部へ取出すことができる。そして、取出した復号化用鍵、暗号化用鍵を別のＩＣカードに書込むことにより、たとえば、バックアップカードを容易に作成できる。

【0099】

したがって、たとえば、内部で生成した復号化用鍵、暗号化用鍵を持つＩＣカードが破壊しても、あらかじめ作成しておいたバックアップカードを用いることにより、該破壊したＩＣカード内の復号化用鍵、暗号化用鍵でデータの隠蔽や正当性の確認が行なわれた電子データファイルを再使用することが可能となる。

【0100】

具体例を用いて更に詳細に説明する。たとえば、図５に示すシステムにおいて、個人端末装置３００と個人端末装置４００との間で電子メールの交換を行なっている場合で、たとえば、ＩＣカード１００aが破損した場合、個人端末装置３００では、過去に個人端末装置４００から送られてきた電子メール、および、新たに個人端末装置４００から送られてきた電子メールを読むことが不可能となる。

【0101】

ところが、前述したようなバックアップカードを用いることにより、個人端末装置３００において、過去に個人端末装置４００から送られてきた電子メールを読むことができ、新しいＩＣカードを取得するまでの間、新たに個人端末装置４００から送られてきた電子メールを読むことや、個人端末装置４００に暗号化した電子メールを送ることが可能となる。

【0102】

なお、前記実施の形態では、鍵１をあらかじめ生成し、個人データベースファイルの一部としてハードディスク装置に格納しておくことで、ＩＣカードを発行する方法を説明したが、よりセキュリティを高めるため、たとえば、パーソナル

コンピュータのプログラム、または、専用の鍵生成装置などでカード発行時に自動的に鍵 1 を生成して、IC カード内に設定する方法でもよい。このようにすれば、ハードディスク装置に格納しないため、セキュリティをより高くすることができる。

【0103】

また、同様に、鍵 2、鍵 3 を画面入力する方法で説明したが、よりセキュリティを高めるため、たとえば、パーソナルコンピュータのプログラム、または、専用の鍵生成装置などでカード発行時に自動的に鍵 2、鍵 3 を生成して、IC カード内に設定する方法でもよい。

【0104】

また、復号化用鍵取出し・設定命令用鍵群の数が 3 つの場合について説明したが、たとえば、鍵 1 のみ、鍵 1 と鍵 2 のみ、あるいは、4 つ以上の鍵としてもよい。

【0105】

また、本カード内にバックアップカード作成フラグを設けて、鍵群を使用して、復号化用鍵、暗号化用鍵が外部へ取出された場合には上記フラグを立て、フラグが立っている場合は鍵を外部へ取出すことができないようにすれば、さらにセキュリティを高めることができる。

【0106】

また、バックアップカードを作成した後は、本カードのデータメモリ内の鍵群エリアを鍵取出し不可とすることにより、鍵を取出すことができないようにしてもよい。

【0107】

また、復号化用鍵取出し・設定命令用鍵群の鍵 1 をカード発行時に、鍵 2 と鍵 3 をバックアップカードの作成時に、それぞれ設定する方法について説明したが、たとえば、図 20 および図 21 に示すように、鍵 1、鍵 2、鍵 3 を全てカード発行時に設定する方法でもよい。すなわち、カード製造者が鍵 1、鍵 2、鍵 3 を全て設定するものである。なお、図 20 は、カード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリ 102 の内部の状態を、図

21 は、ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリ 102 の内部の状態を、それぞれ示している。

【0108】

また、復号化用鍵取出し・設定命令用鍵群の鍵 1 をカード発行時に、鍵 2 と鍵 3 をバックアップカードの作成時に、それぞれ設定する方法について説明したが、たとえば、図 22 および図 23 に示すように、鍵 1、鍵 2、鍵 3 を全てバックアップカードの作成時に設定する方法でもよい。すなわち、ユーザが鍵 1、鍵 2、鍵 3 を全て設定するものである。なお、図 22 は、カード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリ 102 の内部の状態を、図 23 は、ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリ 102 の内部の状態を、それぞれ示している。

【0109】

また、復号化用鍵、暗号化用鍵をバックアップカードの作成時に生成する方法について説明したが、たとえば、図 24 および図 25 に示すように、カード発行時に生成する方法でもよい。すなわち、鍵をカード製造者とユーザが分けて設定するものである。なお、図 24 は、カード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリ 102 の内部の状態を、図 25 は、ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリ 102 の内部の状態を、それぞれ示している。

【0110】

また、復号化用鍵のみをバックアップカードに設定する方法について説明したが、新しい IC カードがユーザに届くまでの間に業務に支障が生じないように、たとえば、図 26 および図 27 に示すように、暗号化用鍵をもバックアップカードカードに設定する方法でもよい。なお、図 26 は、カード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリ 102 の内部の状態を、図 27 は、ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリ 102 の内部の状態を、それぞれ示している。

【0111】

さらに、復号化用鍵、暗号化用鍵を IC カード内で生成する方法について説明

したが、たとえば、図 2 8 に示すように、個人端末装置 3 0 0 および個人端末装置 4 0 0 を通信回線 5 0 0 を介して認証局（鍵を生成するサービスセンタ） 6 0 0 に接続し、認証局 6 0 0 で生成された復号化用鍵、暗号化用鍵を例えば個人端末装置 3 0 0 にダウンロードすることにより、本カード 1 0 0 c に復号化用鍵、暗号化用鍵を設定するようにしてもよい。

【 0 1 1 2 】

この場合の本カード 1 0 0 c およびバックアップカード 1 0 0 d への鍵の設定、本カード 1 0 0 c への暗号化用鍵および復号化用鍵の設定、本カード 1 0 0 c からの復号化用鍵の取出し、バックアップカード 1 0 0 d への復号化用鍵の設定を行なう処理は、図 2 9 に示すフローチャートのようにになる。図 2 9 のフローチャートは、前述した図 1 5 のフローチャートに対し以下の点が若干異なる。すなわち、ステップ S 2 0 4 と S 2 0 5 との間に認証局 6 0 0 から本カード用の復号化用鍵、暗号化用鍵を取得するステップ S 2 0 9 が追加される。また、ステップ S 2 0 5 の処理が本カード用の復号化用鍵、暗号化用鍵設定命令の送信となるとともに、ステップ S 2 0 5 a の処理が復号化用鍵、暗号化用鍵の設定となる。

【 0 1 1 3 】

この場合のカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリ 1 0 2 の内部の状態を図 3 0 に示し、ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリ 1 0 2 の内部の状態を図 3 1 に示している。

【 0 1 1 4 】

【発明の効果】

以上詳述したように本発明によれば、内部に記憶された、データを暗号化あるいは復号化するための鍵を安全に外部へ取出すことのできる IC カードを提供できる。

【 0 1 1 5 】

また、本発明によれば、IC カード内に記憶された、データを暗号化あるいは復号化するための鍵を安全に外部へ取出し、それを別の IC カード内に記憶することにより、その複製カード（たとえば、バックアップカード）を容易に作成す

ることのできる I C カード端末装置および I C カード複製方法を提供できる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態に係る I C カード発行システムの構成例を概略的に示すブロック図。

【図 2】

I C カードの構成例を概略的に示すブロック図。

【図 3】

I C カード側から出力されるレスポンスのフォーマット例を示す図。

【図 4】

I C カードのデータメモリにおけるファイル構造の一例を示す図。

【図 5】

I C カードの鍵を利用するシステムの一例を示すブロック図。

【図 6】

個人データベースファイルの一例を示す構成図。

【図 7】

本カード用の命令コードデータベースファイルの一例を示す構成図。

【図 8】

バックアップカード用の命令コードデータベースファイルの一例を示す構成図

【図 9】

バックアップカード用 I C カードのデータメモリにおけるファイル構造の一例を示す図。

【図 10】

命令データの一例を示す図。

【図 11】

本カードおよびバックアップカードの発行処理を説明するフローチャート。

【図 12】

カード製造者からの出荷状態の本カードおよびバックアップカードにおけるデ

ータメモリの内部状態を模式的に示す図。

【図 1 3】

発行された本カードに暗号化用鍵および復号化用鍵を生成させ、バックアップカードに復号化用鍵を設定するシステムの構成を示すブロック図。

【図 1 4】

鍵入力画面の一例を示す図。

【図 1 5】

本カードおよびバックアップカードへの鍵の設定、本カードでの暗号化用鍵および復号化用鍵の生成、本カードからの復号化用鍵の取出し、バックアップカードへの復号化用鍵の設定を行なう処理を説明するフローチャート。

【図 1 6】

ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図 1 7】

本カードおよびバックアップカードの作成処理の模様を説明する模式図。

【図 1 8】

ファイル名入力画面の一例を示す図。

【図 1 9】

バックアップカードでの電子データファイルの復号化処理、および、新しい本カードでの電子データファイルの暗号化処理を説明するフローチャート。

【図 2 0】

他の例におけるカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図 2 1】

他の例におけるユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図 2 2】

他の例におけるカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図 2 3】

他の例におけるユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図 2 4】

他の例におけるカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図 2 5】

他の例におけるユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図 2 6】

他の例におけるカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図 2 7】

他の例におけるユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図 2 8】

他の例において、発行された本カードに暗号化用鍵および復号化用鍵を設定し、バックアップカードに復号化用鍵を設定するシステムの構成を概略的に示すブロック図。

【図 2 9】

他の例において、本カードおよびバックアップカードへの鍵の設定、本カードへの暗号化用鍵および復号化用鍵の設定、本カードからの復号化用鍵の取出し、バックアップカードへの復号化用鍵の設定を行なう処理を説明するフローチャート。

【図 3 0】

他の例におけるカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図 3 1】

他の例におけるユーザ使用開始前状態の本カードおよびバックアップカードに

おけるデータメモリの内部状態を模式的に示す図。

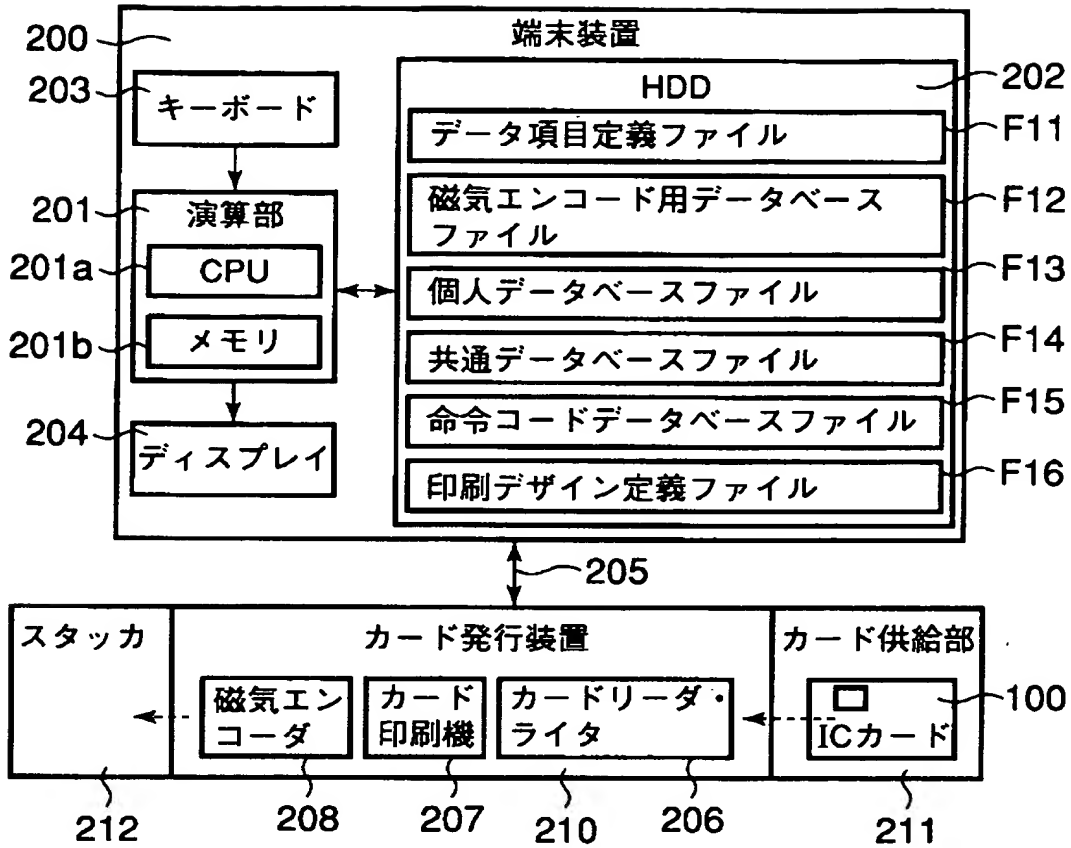
【符号の説明】

1 0 0, 1 0 0 a, 1 0 0 b… I C カード、1 0 0 c…本カード、1 0 0 d…
バックアップカード（複製カード）、1 0 1…制御素子、1 0 2…データメモリ
、1 0 3…ワーキングメモリ、1 0 4…プログラムメモリ、1 0 5…コンタクト
部、1 0 6… I C チップ、2 0 0…端末装置、2 0 1…端末本体、2 0 1 a…C
P U、2 0 1 b…メモリ、2 0 2…ハードディスク装置、2 0 3…キーボード、
2 0 4…ディスプレイ、2 0 6…カードリーダー・ライター、2 0 7…カード印刷機
、2 0 8…磁気エンコーダ、2 1 0…カード発行装置、2 1 1…カード供給部、
2 1 2…カードスタッカ、3 0 0…個人端末装置（I C カード端末装置）、3 0
1…端末本体、3 0 1 a…C P U、3 0 1 b…メモリ、3 0 2…ハードディスク
装置、3 0 3…キーボード、3 0 4…ディスプレイ、3 0 6 a, 3 0 6 b…カー
ドリーダー・ライター、4 0 0…個人端末装置（I C カード端末装置）、4 0 6…カ
ードリーダー・ライター、5 0 0…通信回線。

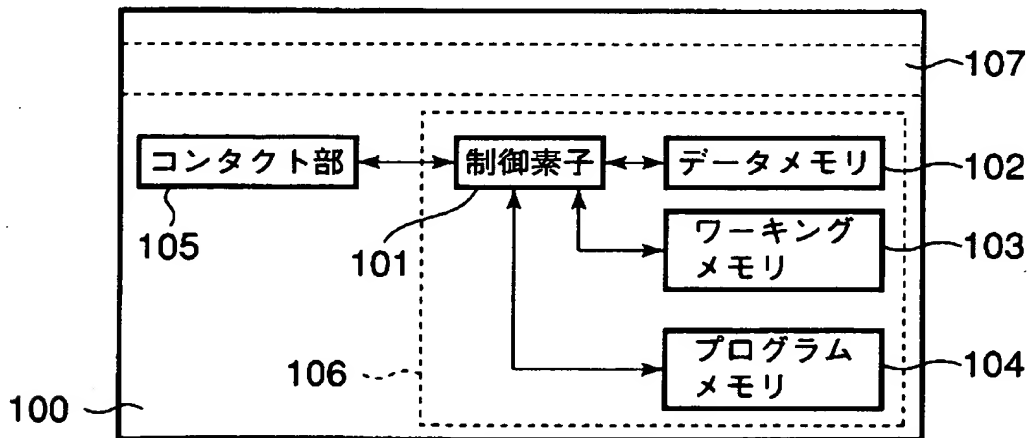
【書類名】

図面

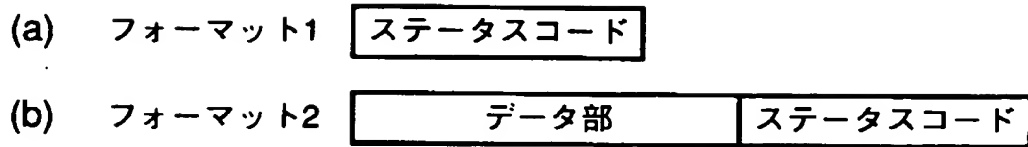
【図 1】



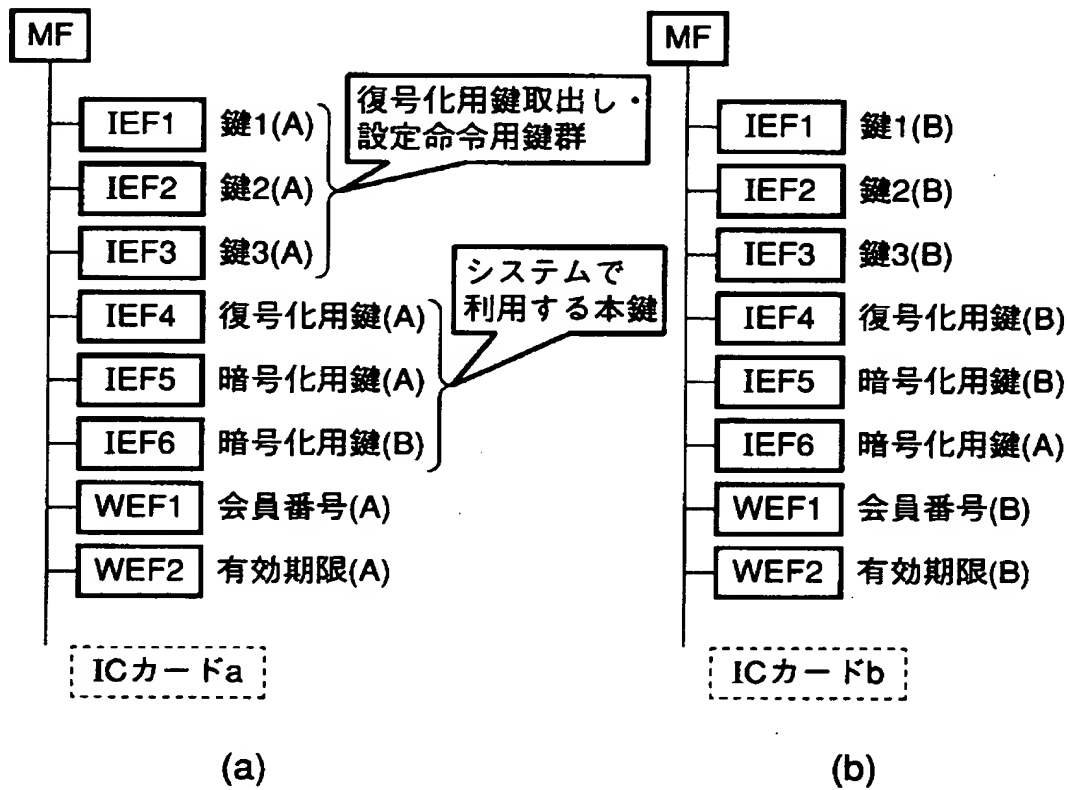
【図 2】



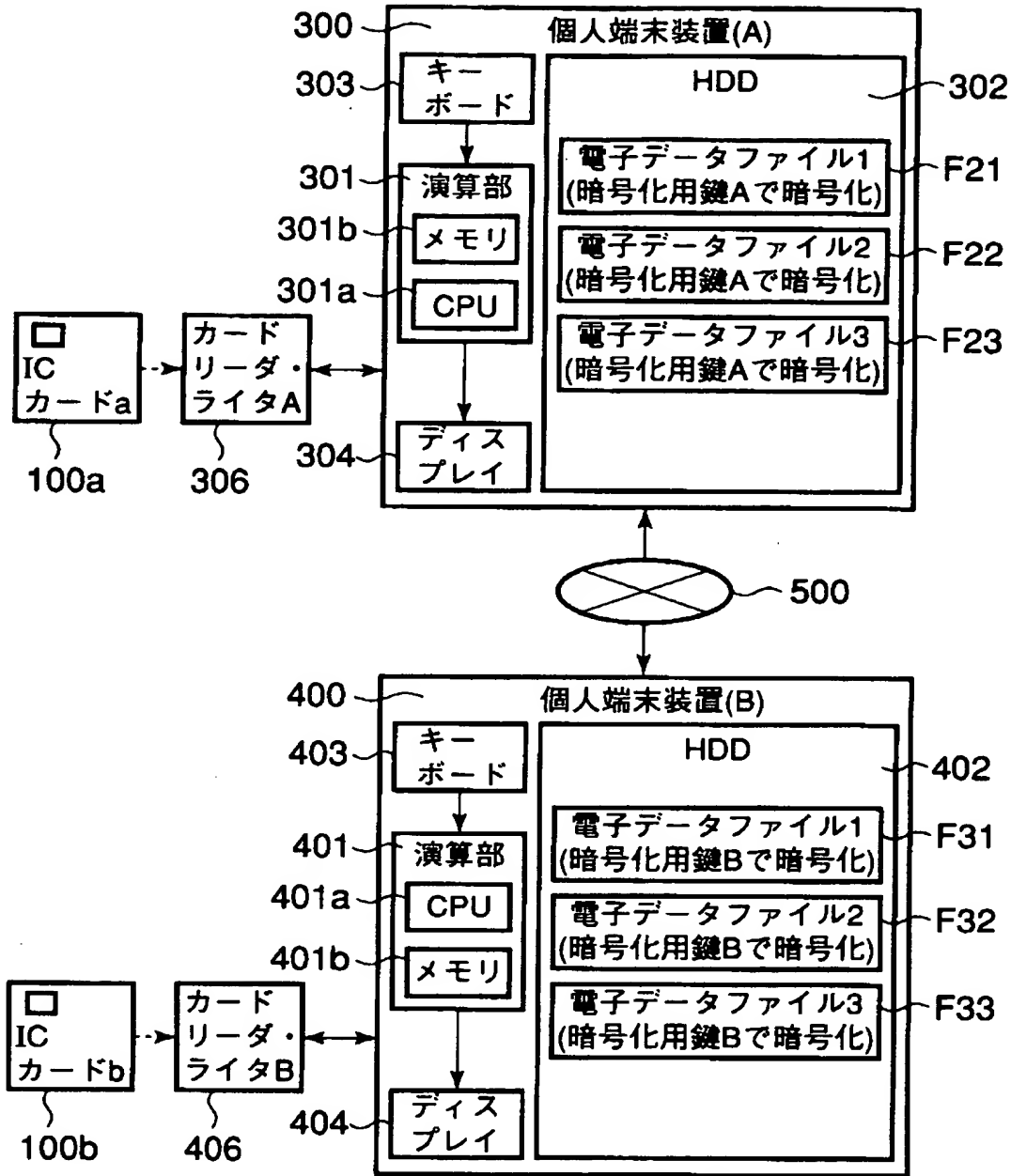
【図 3】



【図 4】



【図 5】



【図 6】

項目1: 漢字氏名	項目2: 漢字住所	項目3: カナ名字	項目4: 会員番号	項目5: 有効期限	項目6: パスワード	項目7: 鍵1
コード#1 田中 太郎	練馬区	TANAKA	000007	2000.09	737c545a87	93 24..d8 88 AB
コード#2 鈴木 次郎	江東区	SUZUKI	000014	2001.10	4787ea7184	d0 93..b2 cb 46
...
...
コード#13 林 三郎	新宿区	HAYASHI	000157	2005.08	c8d7eb567f	82 6a..eb 0b 87
コード#14 松本 四郎	杉並区	MATSUMOTO	000004	2002.07	8181fc35d8	49 83..6c 44 78
...
...
コード#21 中村 五郎	品川区	NAKAMURA	002004	2000.12	eefaac5620	35 89..fb f9 90

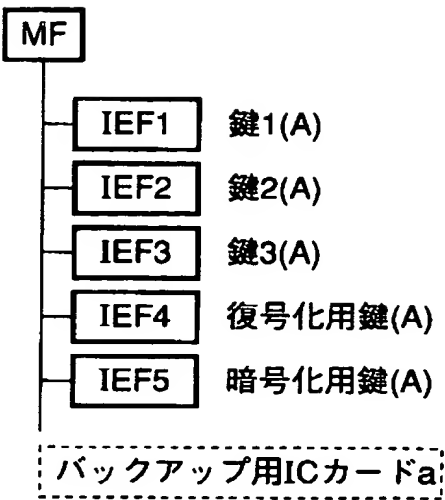
【図 7】

命令コード	命令コードの内容	付加データ	IC出力情報
命令コード1	命令コード1の内容	X	90 00
命令コード2	命令コード2の内容	X	90 00
...
命令コード18	命令コード18の内容	個別ファイル：項目6	90 00
命令コード19	命令コード19の内容	個別ファイル：項目7	90 00
命令コード20	命令コード20の内容	X	90 00
...
命令コード25	命令コード25の内容	個別ファイル：項目5	90 00
...
命令コード30	命令コード30の内容	X	90 00
命令コード31	命令コード31の内容	X	90 00
...

【図 8】

命令コード	命令コードの内容	付加データ	IC出力情報
命令コード1	命令コード1の内容	×	90 00
命令コード2	命令コード2の内容	×	90 00
...
...
命令コード18	命令コード18の内容	個別ファイル：項目6	90 00
命令コード19	命令コード19の内容	個別ファイル：項目7	90 00

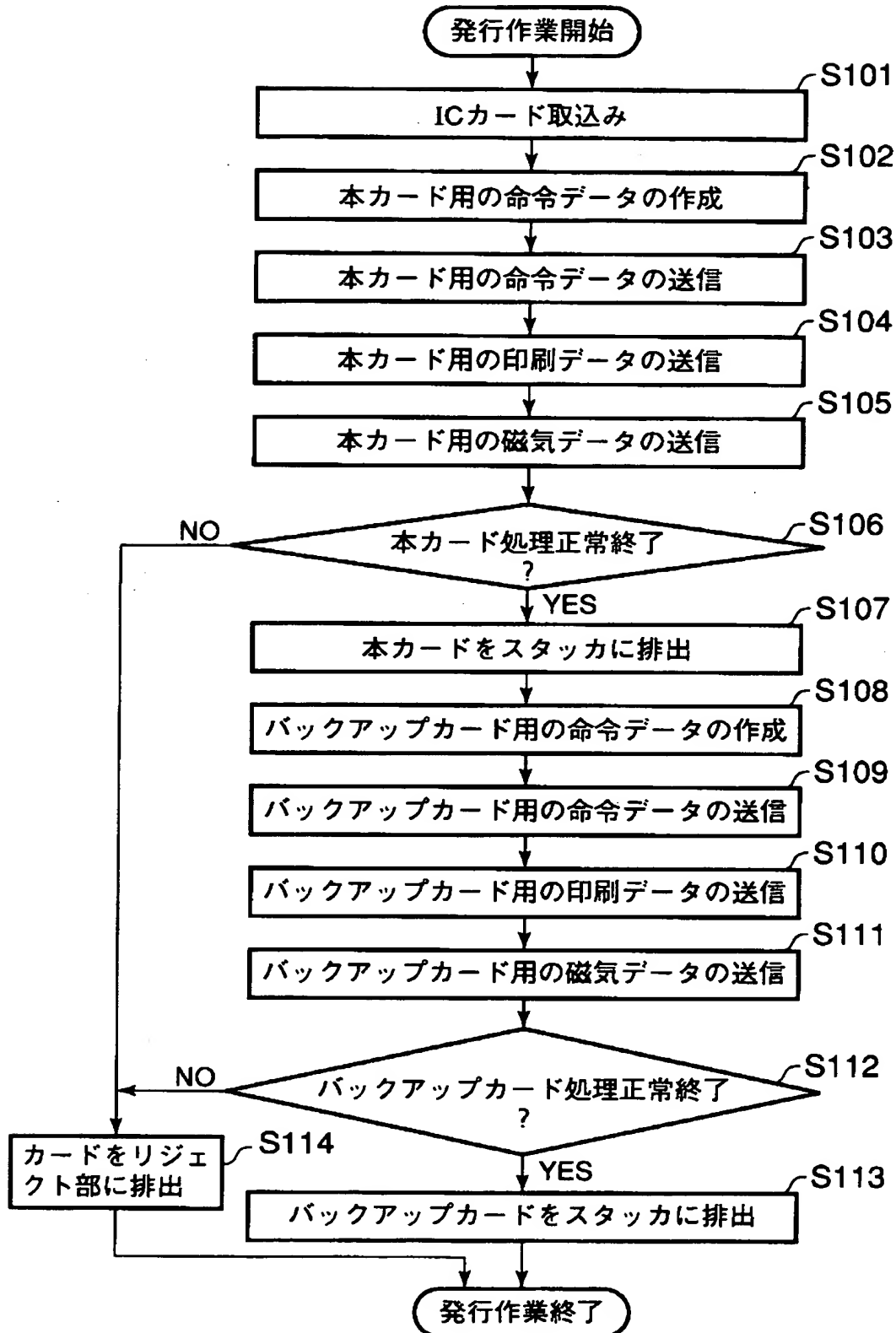
【図 9】



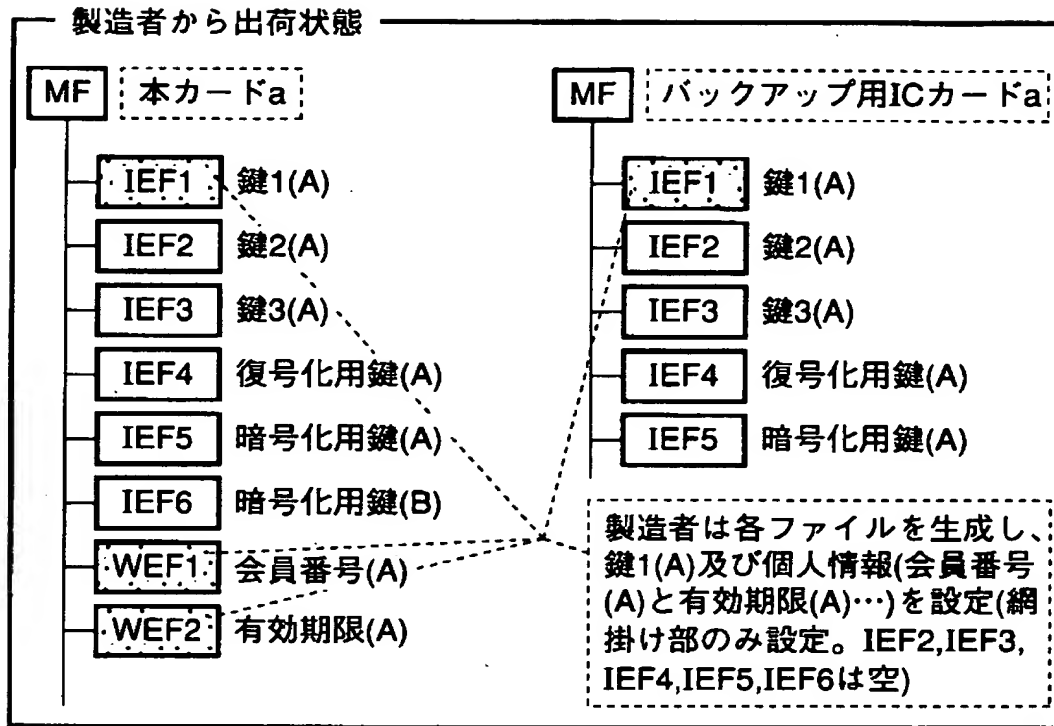
【図 1 0】

付加データ	
命令コード19の内容	49 83..6c 44 78

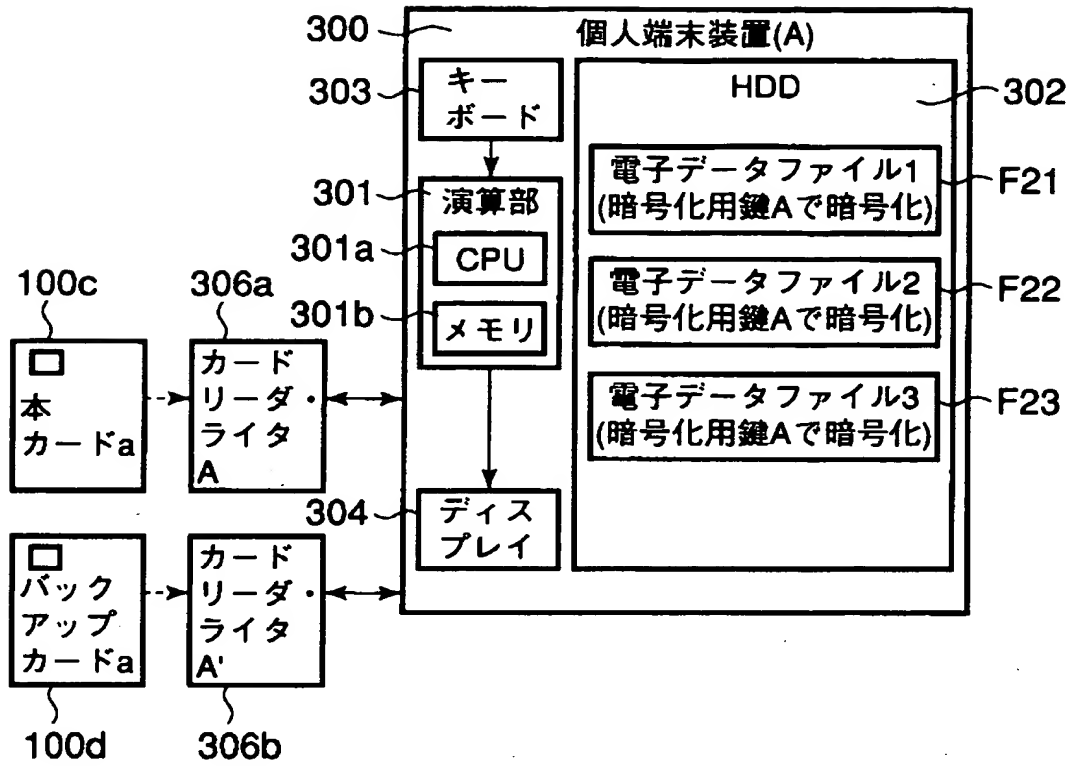
【図 1 1】



【図 1 2】



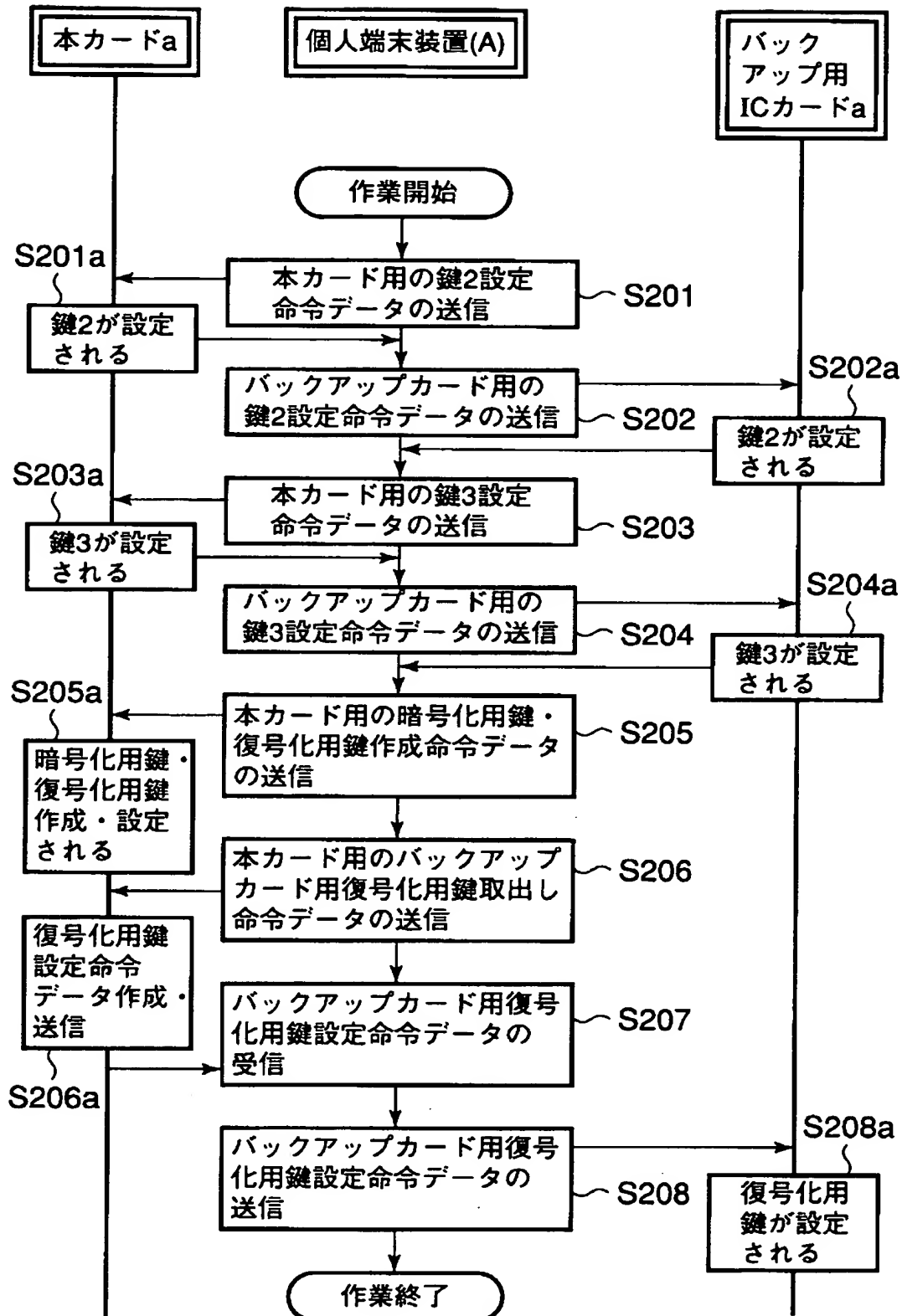
【図 1 3】



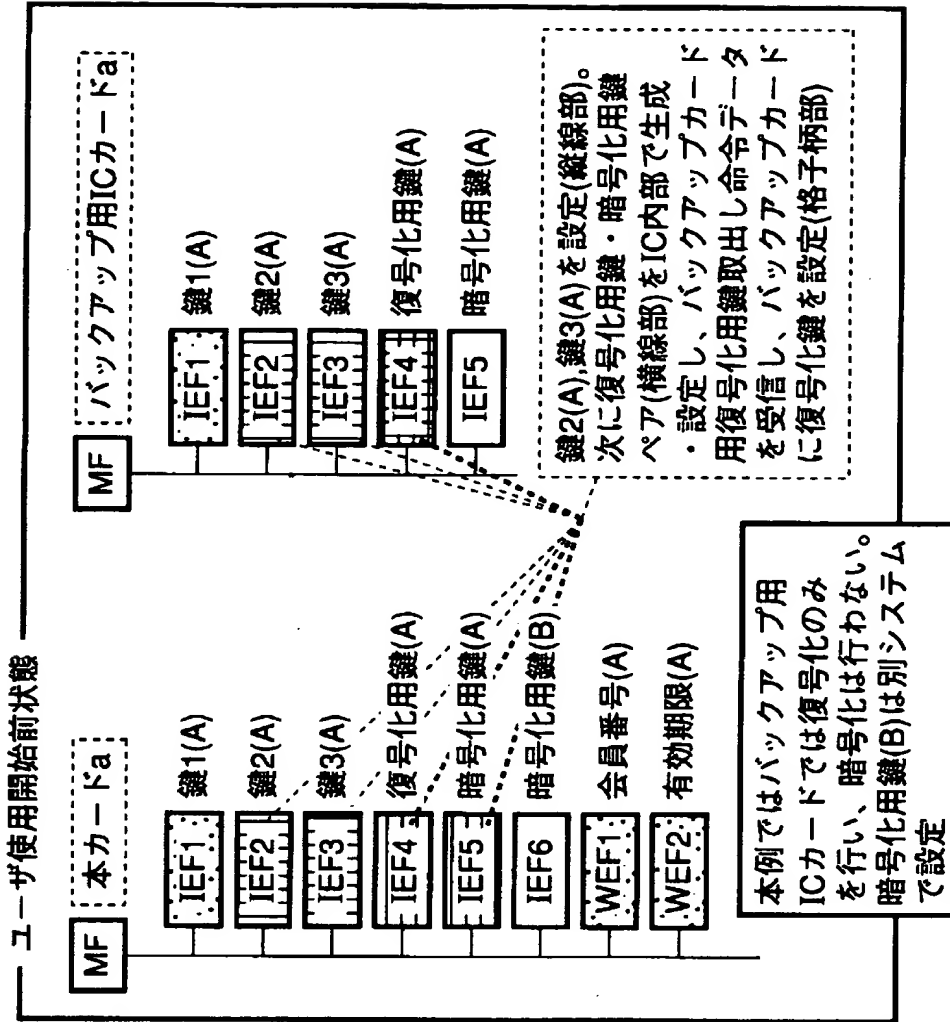
【図 1 4】

鍵2・3入力画面	
パスワードと鍵2・3を入力して下さい。	
パスワード	<input type="text"/>
鍵2	<input type="text"/>
鍵3	<input type="text"/>
<input type="button" value="入力終了"/> <input type="button" value="終了"/>	

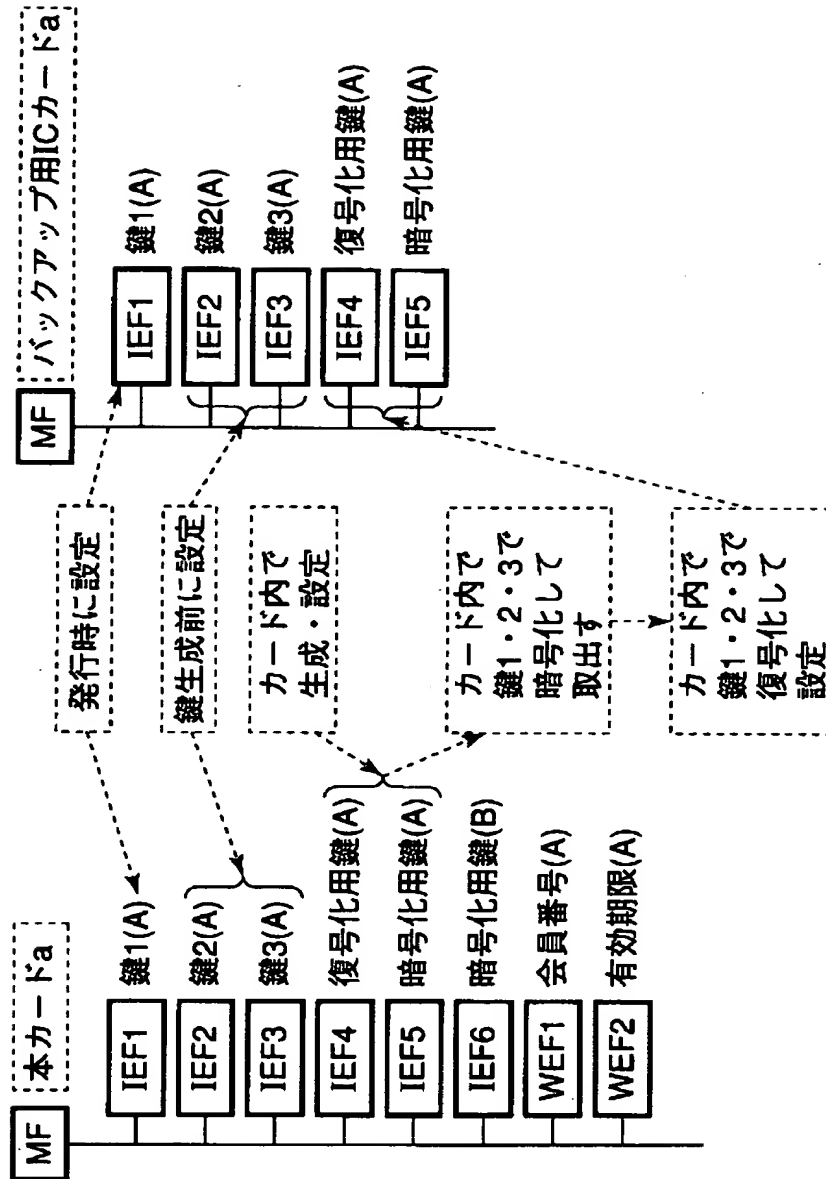
【図15】



【図 16】



【図 17】



【図 18】

ファイル名入力画面

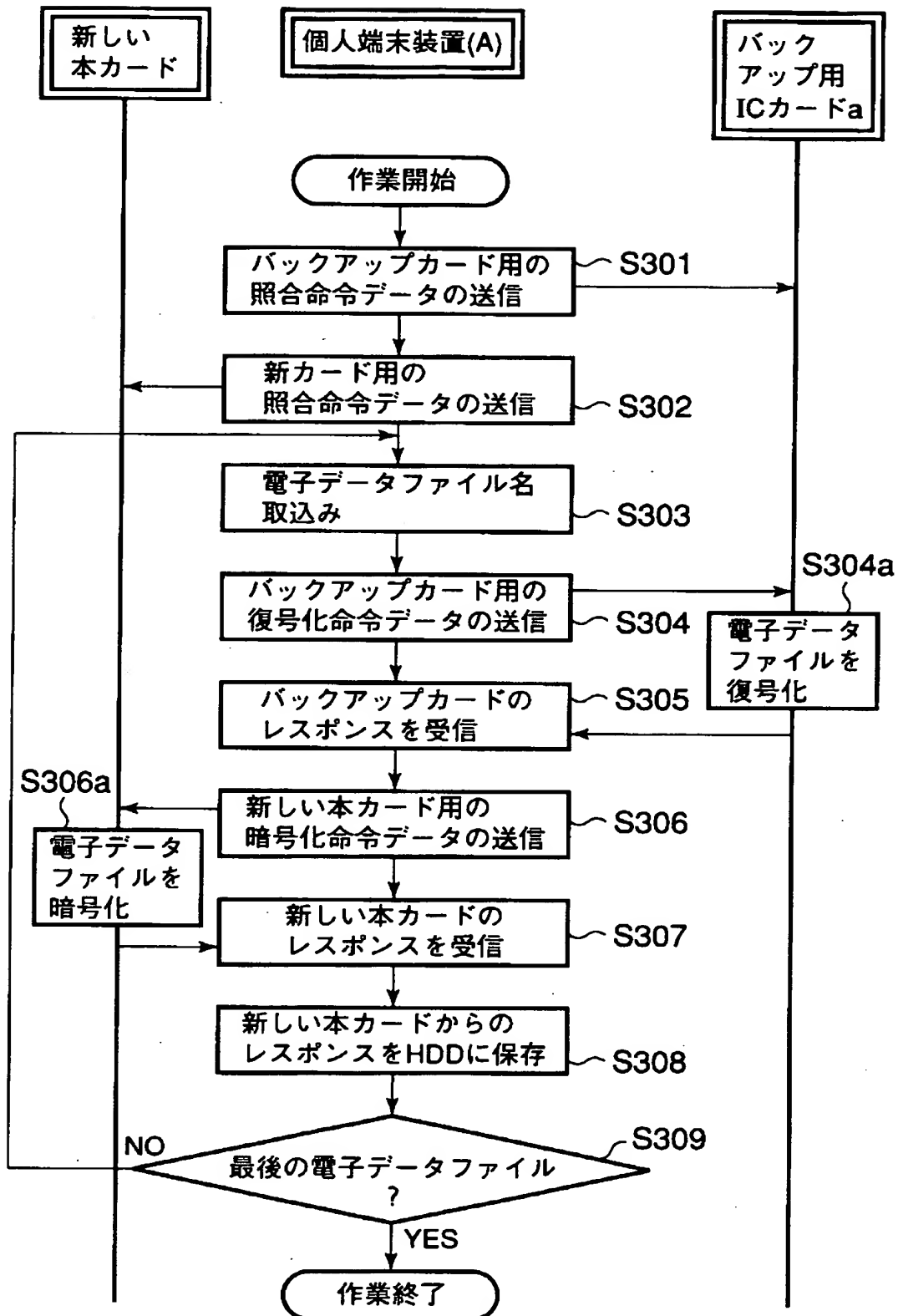
パスワードと新カードで暗号化するファイル名を入力して下さい。

バックアップカードのパスワード

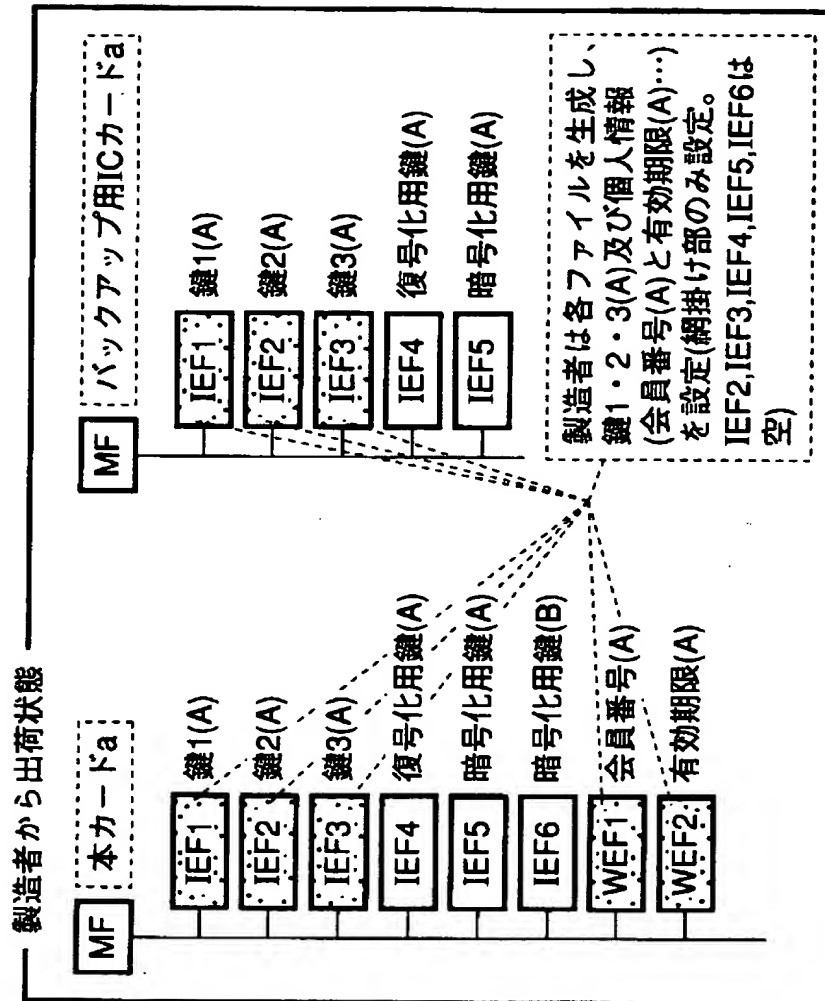
新カードのパスワード

名前	フォルダ名
電子データファイル1.dat	c:\filebox
電子データファイル2.txt	c:\filebox1
電子データファイル3.bin	c:\filebox2

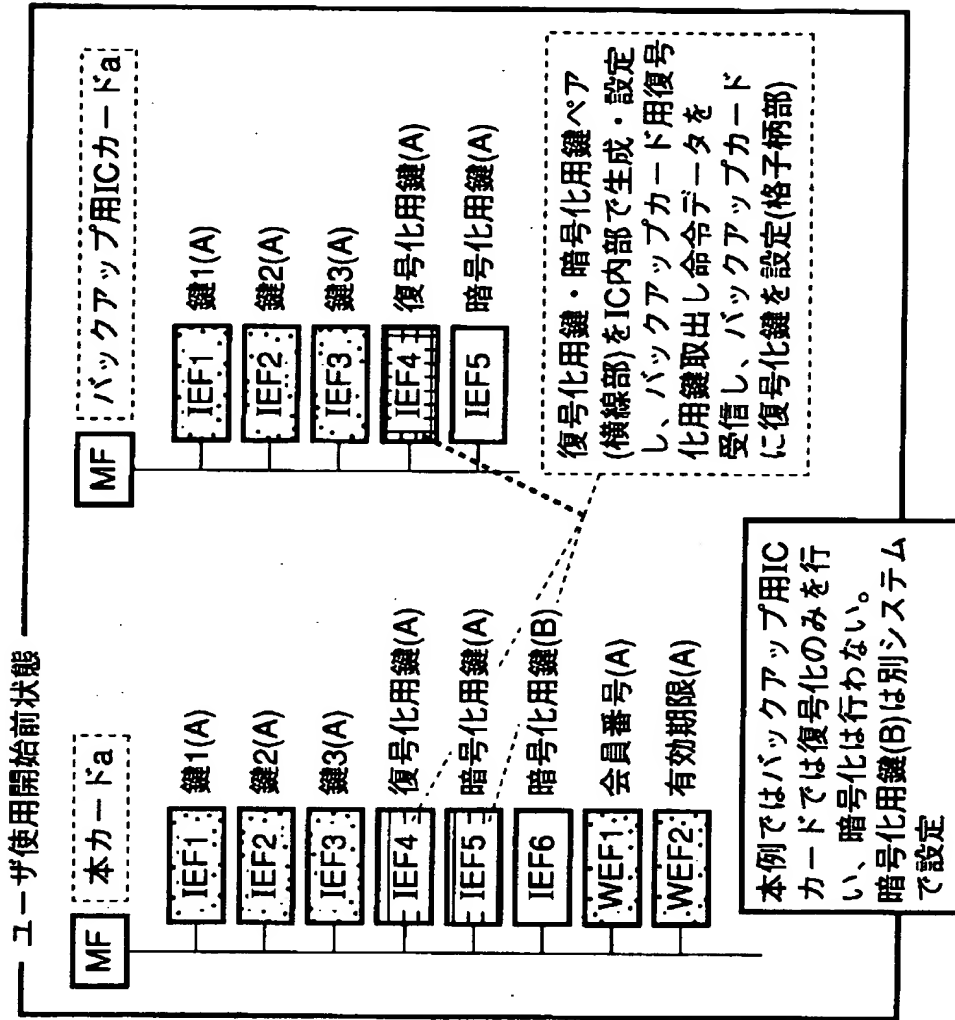
【図19】



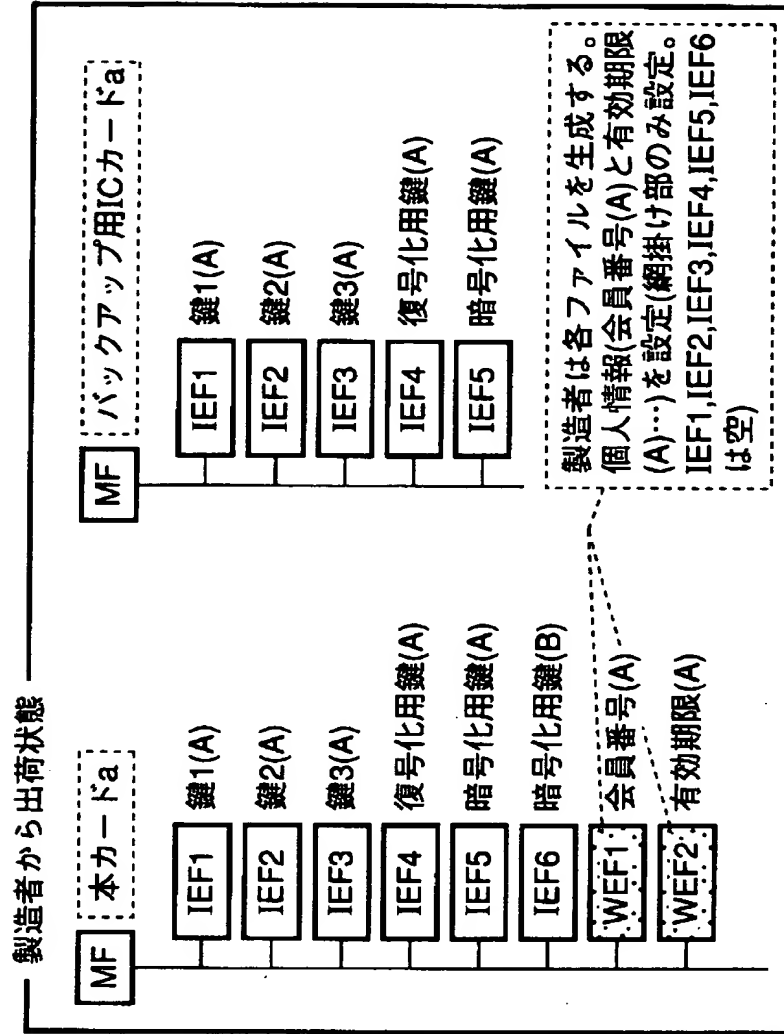
【図 20】



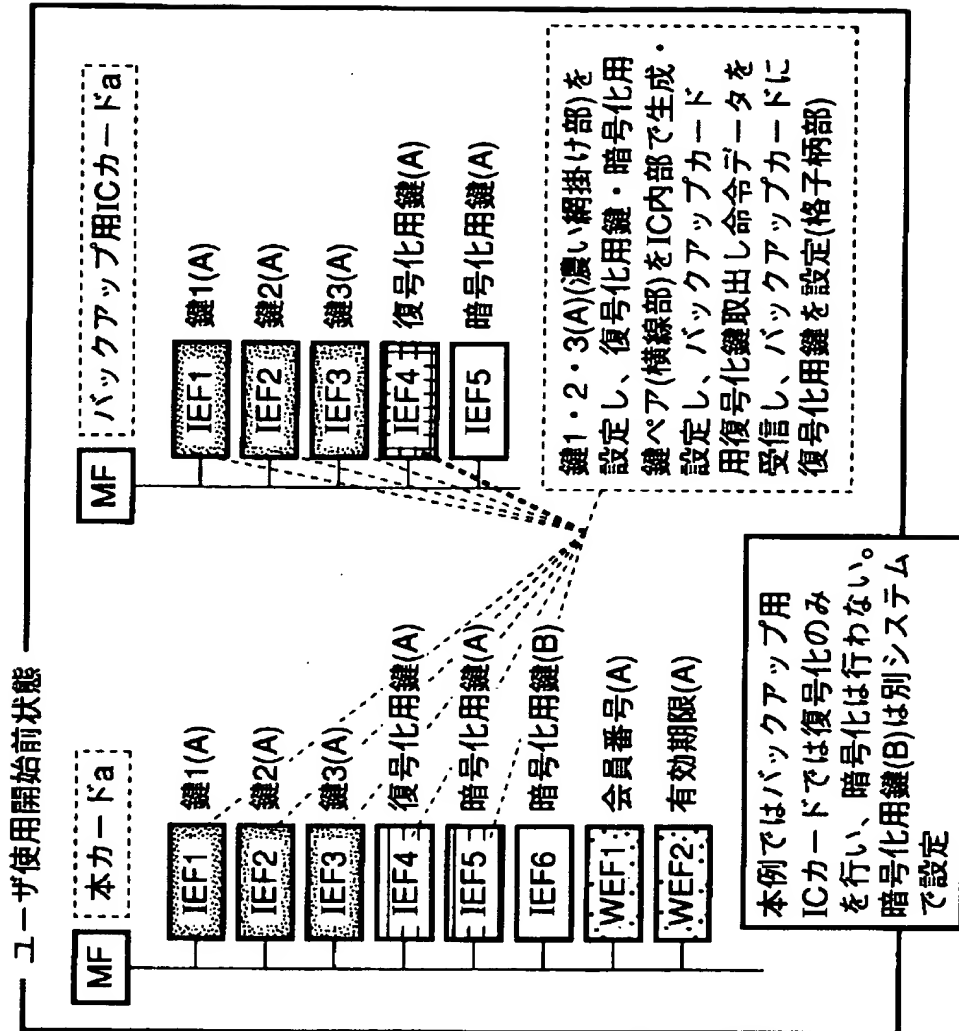
【図 21】



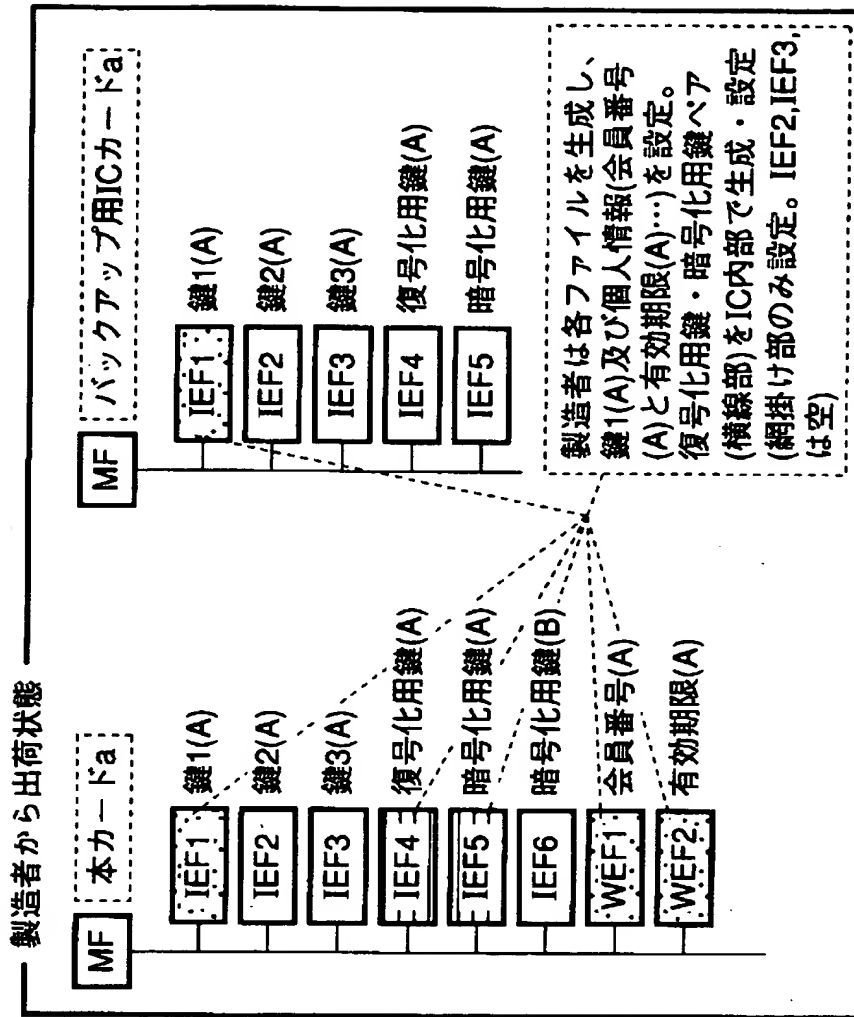
【図 2 2】



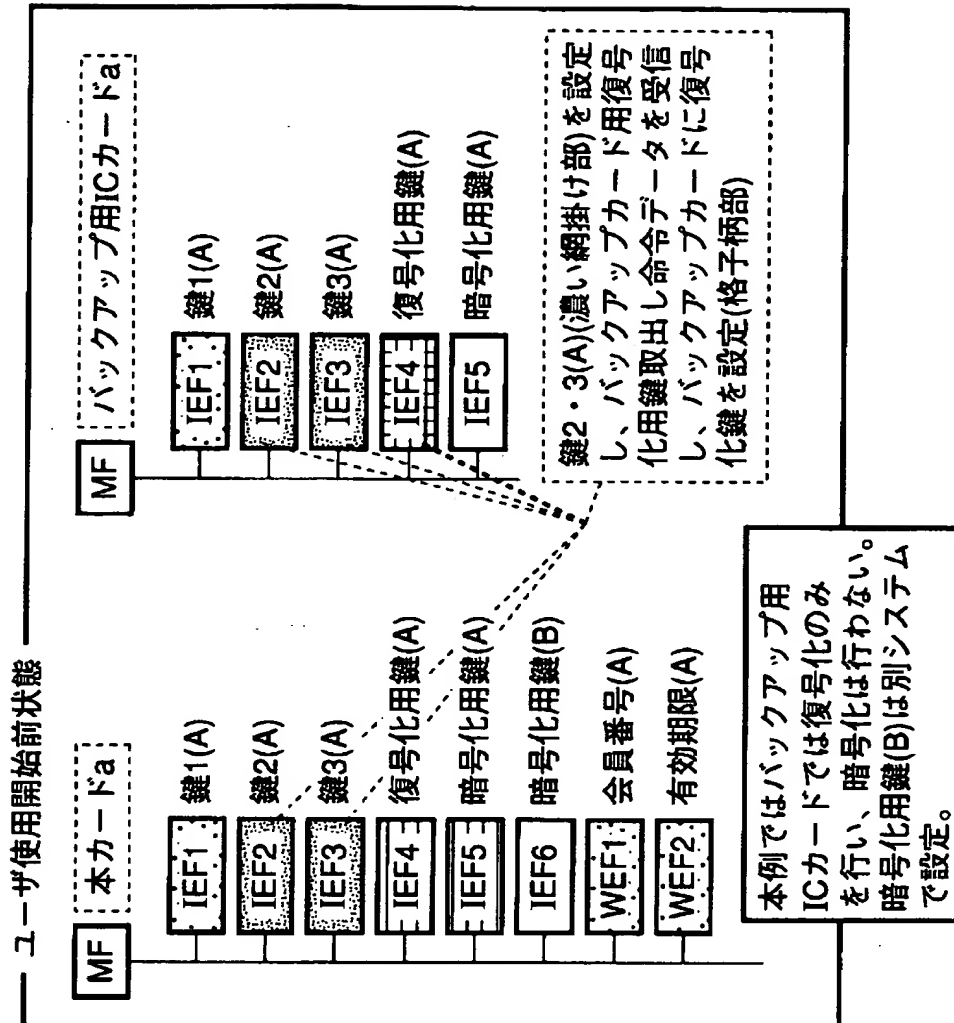
【図 2 3】



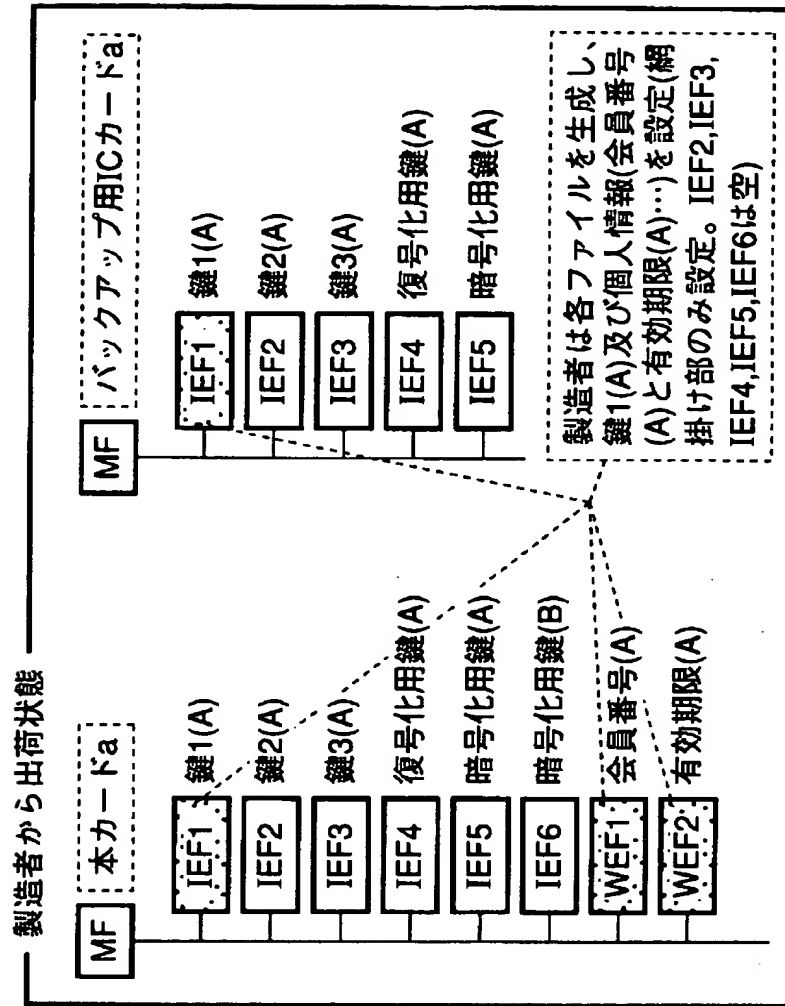
【図 2 4】



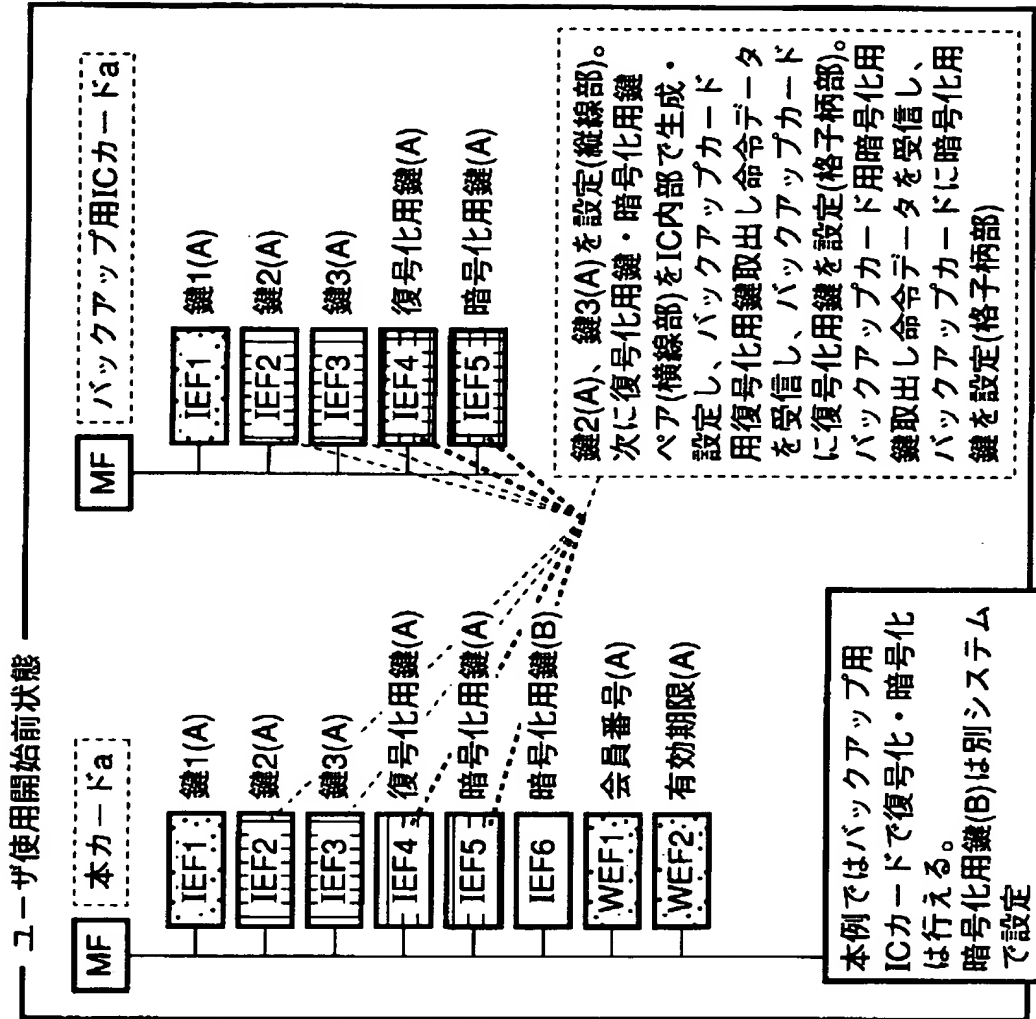
【図 25】



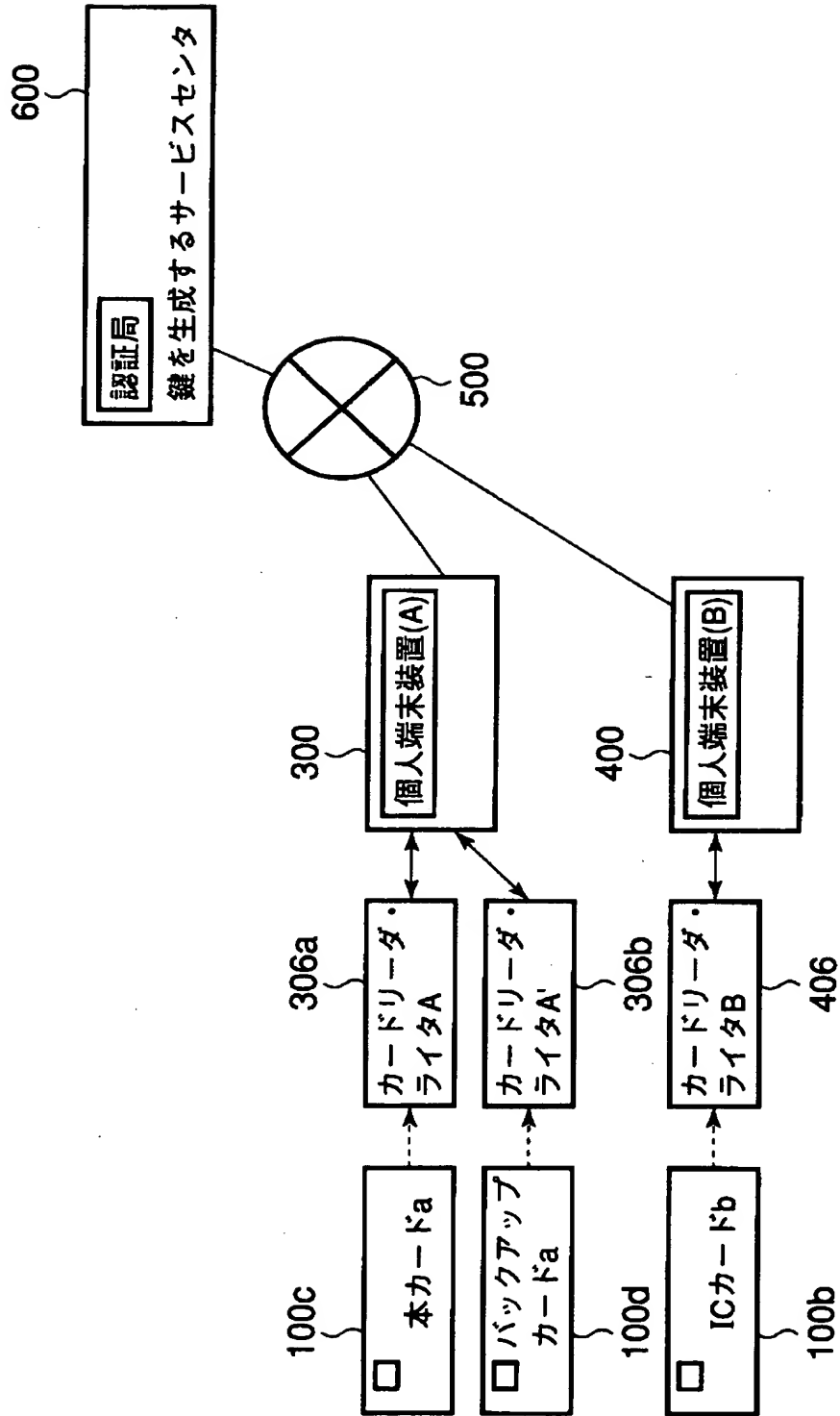
【図 2 6】



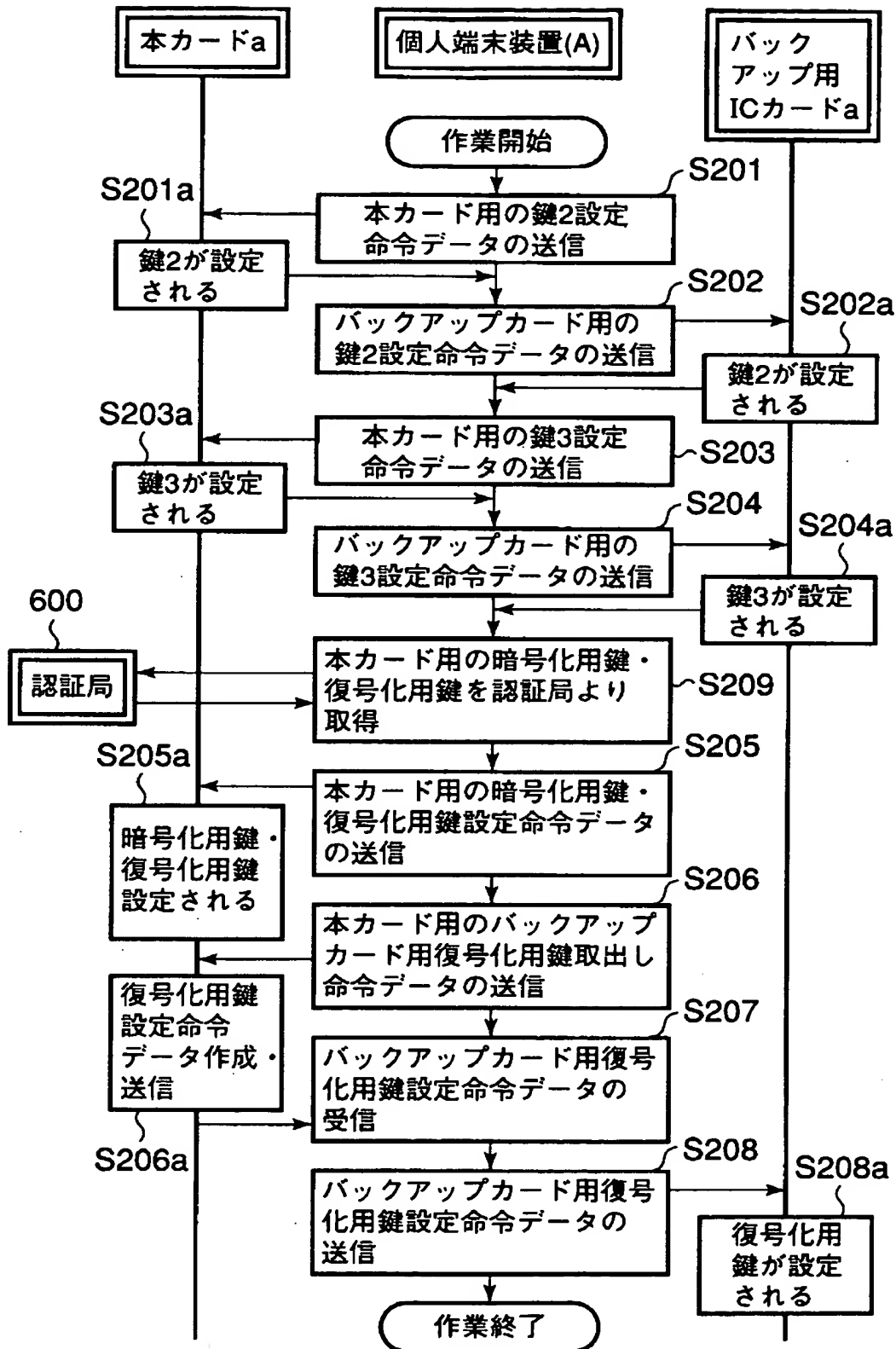
【図 27】



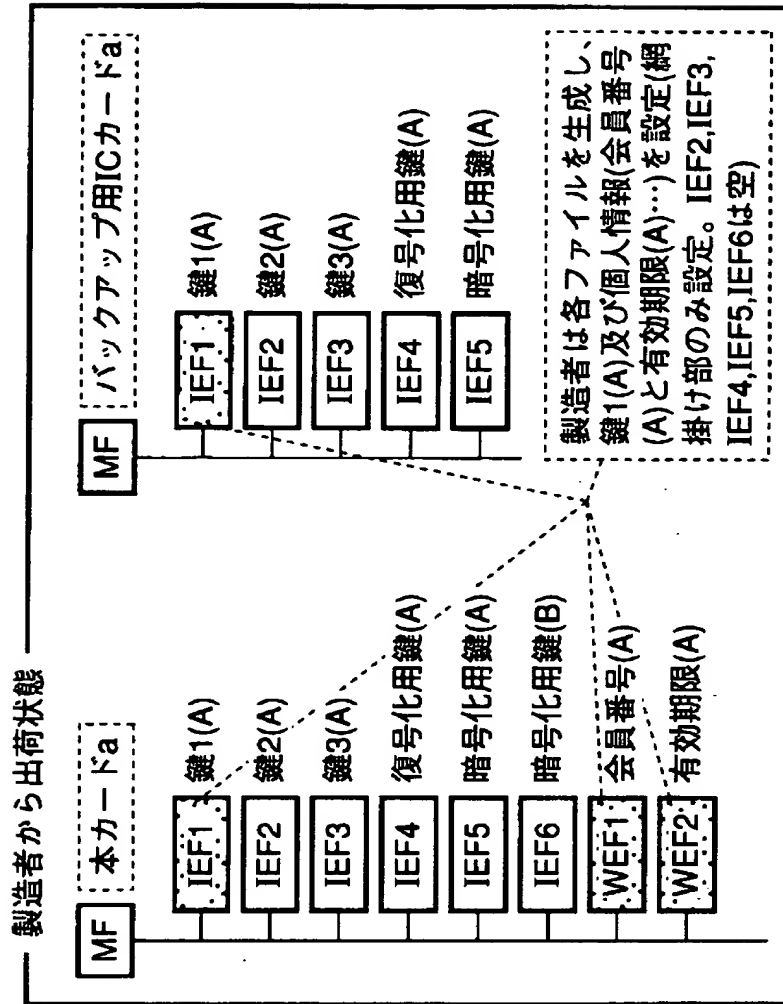
【図 28】



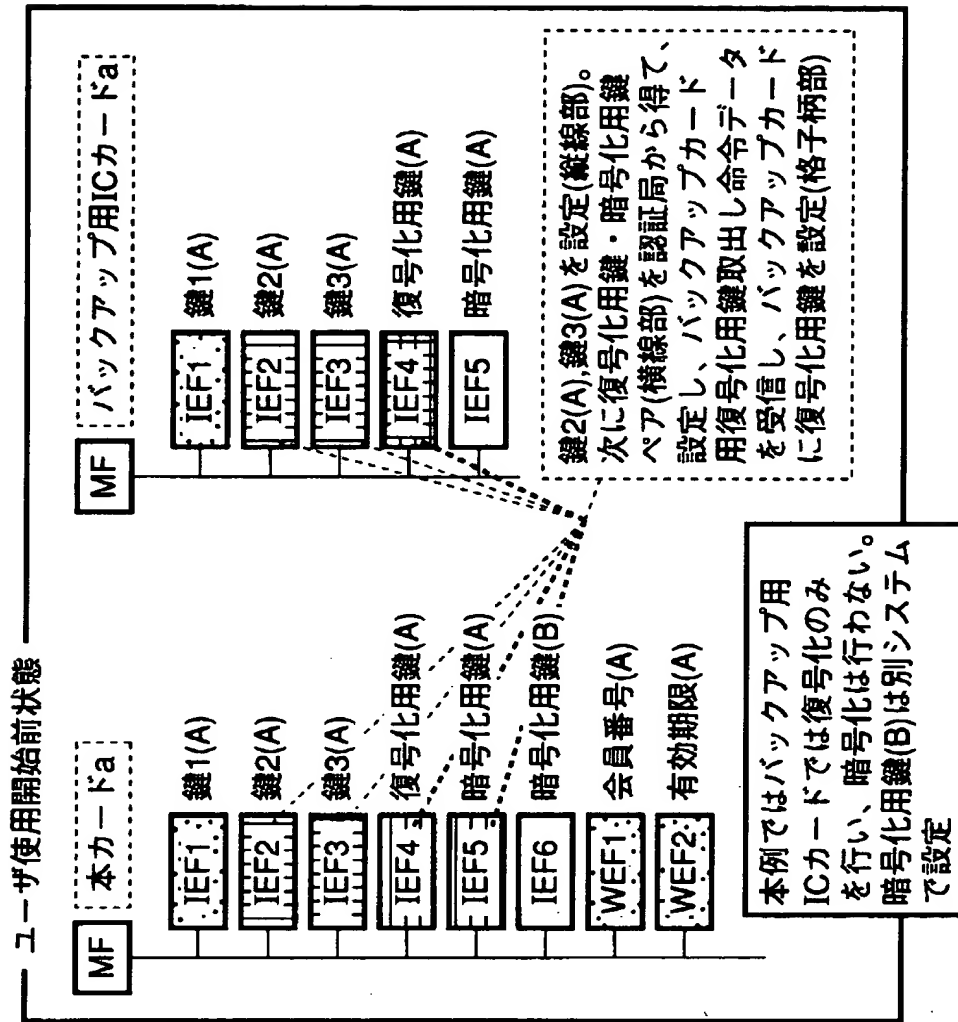
【図 29】



【図 3 0】



【図 3 1】



【書類名】 要約書

【要約】

【課題】 内部に記憶された、データを暗号化あるいは復号化するための鍵を安全に外部へ取出すことのできる I C カードを提供する。

【解決手段】 内部で生成あるいは外部から設定された、データを復号化するための復号化用鍵、データを暗号化するための暗号化用鍵を持つ I C カードにおいて、I C カード内の復号化用鍵、暗号化用鍵を外部へ取出すための鍵取出命令が入力された場合、該 I C カード内に設定された別の複数の鍵で復号化用鍵、暗号化用鍵を暗号化してから外部へ送出する。

【選択図】 図 1 5

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日 1990年 8月22日
[変更理由] 新規登録
住 所 神奈川県川崎市幸区堀川町72番地
氏 名 株式会社東芝